

Nos. 23-13698-E

**UNITED STATES COURT OF APPEALS
FOR THE ELEVENTH CIRCUIT**

COIN CENTER, et al.,
Plaintiffs-Appellees,

v.

SECRETARY, U.S. DEPARTMENT OF THE TREASURY, et al.,
Defendants-Appellants.

Appeal from the U.S. District Court for the Northern District of Florida,
No. 3:22-cv-20375-TKW-ZCB (Wetherell, J.)

**APPENDIX OF APPELLANTS COIN CENTER, ET AL.
VOL. 1 of 3**

J. Abraham Sutherland
106 Connally Street
Black Mountain, NC 28711
(805) 689-4577

Jeffrey M. Harris
Cameron T. Norris
Jeffrey S. Hetzel
CONSOVOY MCCARTHY PLLC
1600 Wilson Boulevard, Suite 700
Arlington, Virginia 22209
(703) 243-9423
cam@consovoymccarthy.com

Counsel for Coin Center et al.

CASE NO. 23-13698**INDEX TO DOCUMENT REFERENCES IN APPENDIX**

<u>Description of Item</u>	<u>Record Entry No.</u>	<u>Appendix Tab No.</u>
<u>VOLUME 1</u>		
DISTRICT COURT DOCKET SHEET		
Case No. 3:22-cv-20375-TKW-ZCB	N/A	DKT
FIRST AMENDED COMPLAINT		
(12/08/2022)	R.9	9
ANSWER		
(01/09/2023)	R.17	17
PLAINTIFFS' MOTION FOR SUMMARY JUDGMENT		
(05/26/2023)	R.36	36
<u>Exhibit A</u>		
DECLARATION OF PATRICK O'SULLIVAN.....	R.36-2	
<u>Exhibit B</u>		
DECLARATION OF JOHN DOE	R.36-3	
<u>Exhibit C</u>		
DECLARATION OF DAVID HOFFMAN	R.36.4	
<u>Exhibit D</u>		
DECLARATION OF JERRY BRITO, EXECUTIVE DIRECTOR OF COIN CENTER.....	R.36-5	

<u>Description of Item</u>	<u>Record Entry No.</u>	<u>Appendix Tab No.</u>
JOINT APPENDIX OF ADMINISTRATIVE RECORD DOCUMENTS CITED IN PARTIES' CROSS-MOTIONS FOR SUMMARY JUDGMENT (08/18/2023)	R.68	68

JOINT APPENDIX VOLUME I..... R.68-1

**Designation and Blocking Memorandum
A.R. 1-5**

**Press Release
A.R. 9-12**

**Evidentiary Memorandum
A.R. 13-100**

VOLUME 2

**Exhibit 6: CoinDesk, *Tornado Cash Co-Founder Says the Mixer Protocol is Unstoppable*
A.R. 137-149**

**Exhibit 7: Decrypt.co, *Tornado Cash Ethereum Token Down 50% After Sanctions*
A.R. 150-157**

**Exhibit 15: Medium, *Tornado Cash Introduces Arbitrary Amounts & Shielded Transfers*
A.R. 184-189**

<u>Description of Item</u>	<u>Record Entry No.</u>	<u>Appendix Tab No.</u>
Exhibit 54: Department of the Treasury, <i>Treasury Takes Robust Actions to Counter Ransomware</i> A.R. 474-479		
Exhibit 58: Ethereum, <i>Ethereum Accounts</i> A.R. 505-513		
Exhibit 59: Chainalysis, <i>Dissecting the DAO: Web3 Ownership is Surprisingly Complicated</i> A.R. 514-525		
Exhibit 62: Coin Center, <i>How Does Tornado Cash Work?</i> A.R. 544-576		
Exhibit 63: Chainalysis, <i>Crypto Mixers and AML Compliance</i> A.R. 577-582		
Exhibit 72: FIOD, <i>Arrest of Suspected Developer of Tornado Cash</i> A.R. 629-631		
Exhibit 86: GitHub, <i>Tornado Repositories/ Tornado Classic UI</i> A.R. 714-716		
Exhibit 89: Crypto.com, <i>Crypto Tokens vs. Coins – What’s the Difference?</i> A.R. 727-737		
Exhibit 103: Ethereum, <i>Intro to Ethereum</i> A.R. 814-821		

<u>Description of Item</u>	<u>Record Entry No.</u>	<u>Appendix Tab No.</u>
Exhibit 107: Ethereum, <i>Transactions</i> A.R. 856-872		
Exhibit 108: Certik, <i>What is Blockchain Analysis?</i> A.R. 873-883		
JOINT APPENDIX VOLUME II.....	R.68-2	
Exhibit 120: Tornado Cash, <i>Introduction</i> A.R. 950-954		
Exhibit 130: National Institute of Standards and Technology, <i>Blockchain Technology Overview</i> A.R. 1030-1152		
Exhibit 157: Ethereum, <i>Decentralized Autonomous Organizations</i> A.R. 1312-1322		
<u>VOLUME 3</u>		
Exhibit 175: Immunefi, <i>Tornado Cash Bug Bounties</i> A.R. 1577-1593		
Exhibit 176: Crypto News Australia, <i>Tornado Cash Token (TORN) Surges 94% Following Bullish Protocol Updates</i> A.R. 1594-1599		
Exhibit 179: Attorney General's Cyber Digital Task Force, <i>Cryptocurrency Enforcement Framework</i> A.R. 1752-1835		

<u>Description of Item</u>	<u>Record Entry No.</u>	<u>Appendix Tab No.</u>
Exhibit 184: BeinCrypto, <i>Ethereum Name Service (ENS): Everything You Need to Know</i> A.R. 1931-1944		
Exhibit 199: Harvard Law School Forum on Corporate Governance, <i>An Introduction to Smart Contracts and Their Potential and Inherent Limitations</i> A.R. 2140-2149		
ORDER ON CROSS-MOTIONS FOR SUMMARY JUDGMENT (10/30/2023)	R.74	74
JUDGMENT (10/30/2023)	R.75	75

DOCKET

CLOSED, APPEAL

**U.S. District Court
Northern District of Florida (Pensacola)
CIVIL DOCKET FOR CASE #: 3:22-cv-20375-TKW-ZCB**

COIN CENTER et al v. YELLEN et al

Assigned to: JUDGE T KENT WETHERELL II

Referred to: MAGISTRATE JUDGE ZACHARY C BOLITHO

Demand: \$0

Case in other court: ELEVENTH CIRCUIT COURT OF
APPEALS, 23-13698-E

Cause: 05:551 Administrative Procedure Act

Date Filed: 10/12/2022

Date Terminated: 10/30/2023

Jury Demand: None

Nature of Suit: 899 Other Statutes:

Administrative Procedures Act/Review or
Appeal of Agency Decision

Jurisdiction: U.S. Government Defendant

Plaintiff**COIN CENTER**

represented by **JEFFREY HETZEL**
CONSOVOY MCCARTHY PLLC -
ARLINGTON VA
1600 WILSON BOULEVARD
SUITE 700
ARLINGTON, VA 22209
703-243-9423
Email: jhetzel@consovoymccarthy.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

CAMERON THOMAS NORRIS
CONSOVOY MCCARTHY PLLC -
ARLINGTON VA
1600 WILSON BOULEVARD
SUITE 700
ARLINGTON, VA 22209
703-243-9423
Email: cam@consovoymccarthy.com
ATTORNEY TO BE NOTICED

JEFFREY MATTHEW HARRIS
CONSOVOY MCCARTHY PLLC -
ARLINGTON VA
1600 WILSON BOULEVARD
SUITE 700
ARLINGTON, VA 22209
703-243-9423
Email: jeff@consovoymccarthy.com
ATTORNEY TO BE NOTICED

MICHAEL ADAM SASSO
MICHAEL C SASSO PA - WINTER PARK
FL

10311 W MORSE BLVD
STE 120
WINTER PARK, FL 32789
407-644-7161
Fax: 407-629-6727
Email: notice@sasso-law.com
ATTORNEY TO BE NOTICED

Plaintiff**PATRICK O'SULLIVAN**

represented by **JEFFREY HETZEL**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

CAMERON THOMAS NORRIS
(See above for address)
ATTORNEY TO BE NOTICED

JEFFREY MATTHEW HARRIS
(See above for address)
ATTORNEY TO BE NOTICED

MICHAEL ADAM SASSO
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff**JOHN DOE**

represented by **JEFFREY HETZEL**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

CAMERON THOMAS NORRIS
(See above for address)
ATTORNEY TO BE NOTICED

JEFFREY MATTHEW HARRIS
(See above for address)
ATTORNEY TO BE NOTICED

MICHAEL ADAM SASSO
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff**DAVID HOFFMAN**

represented by **JEFFREY HETZEL**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

CAMERON THOMAS NORRIS
(See above for address)
ATTORNEY TO BE NOTICED

~~JEFFREY MATTHEW HARRIS~~

(See above for address)

*ATTORNEY TO BE NOTICED***MICHAEL ADAM SASSO**

(See above for address)

ATTORNEY TO BE NOTICED

V.

Defendant**JANET YELLEN***IN HER OFFICIAL CAPACITY AS
SECRETARY OF THE TREASURY*

represented by **CHRISTINE L COOGLE**
DOJ-CIV
FEDERAL PROGRAMS BRANCH
1100 L STREET NW
WASHINGTON, DC 20005
202-880-0282
Email: christine.l.coogle@usdoj.gov
ATTORNEY TO BE NOTICED

CHRISTOPHER ROBERT HEALY

DOJ-CIV

1100 L STREET NW
WASHINGTON, DC 20530
202-514-8095

Email: christopher.healy@usdoj.gov
ATTORNEY TO BE NOTICED

Defendant**DEPARTMENT OF THE TREASURY**

represented by **CHRISTINE L COOGLE**
(See above for address)
ATTORNEY TO BE NOTICED

CHRISTOPHER ROBERT HEALY

(See above for address)

*ATTORNEY TO BE NOTICED***Defendant****ANDREA M GACKI***IN HER OFFICIAL CAPACITY AS
DIRECTOR OF THE OFFICE OF
FOREIGN ASSETS CONTROL*

represented by **CHRISTINE L COOGLE**
(See above for address)
ATTORNEY TO BE NOTICED

CHRISTOPHER ROBERT HEALY

(See above for address)

*ATTORNEY TO BE NOTICED***Defendant****OFFICE OF FOREIGN ASSETS
CONTROL**

represented by **CHRISTINE L COOGLE**
(See above for address)
ATTORNEY TO BE NOTICED

CHRISTOPHER ROBERT HEALY

*ATTORNEY TO BE NOTICED***Amicus****ANDREESSEN HOROWITZ**

represented by **ALESSIO EVANGELISTA**
SKADDEN ARPS ETC LLP -
WASHINGTON DC
1440 NEW YORK AVENUE NW
WASHINGTON, DC 20005
202-371-7170
Email: alessio.evangelista@skadden.com
ATTORNEY TO BE NOTICED

JESSIE K LIU
SKADDEN ARPS ETC LLP -
WASHINGTON DC
1440 NEW YORK AVENUE NW
WASHINGTON, DC 20005
202-371-7000
Fax: 202-661-2340
Email: jessie.liu@skadden.com
ATTORNEY TO BE NOTICED

Amicus**Paradigm Operations LP**

represented by **KATHERINE C YARGER**
LEHOTSKY KELLER COHN LLP -
DENVER CO
700 COLORADO BOULEVARD
UNIT 407
DENVER, CO 80206
303-717-4749
Email: katie@lkcfirm.com
ATTORNEY TO BE NOTICED

RODRIGO SEIRA
PARADIGM - SAN FRANCISCO CA
584 MARKET STREET
SAN FRANCISCO, CA 94104
303-718-1999
Email: rodrigo@paradigm.xyz
ATTORNEY TO BE NOTICED

Amicus**BLOCKCHAIN ASSOCIATION**

represented by **BRIAN CHARLES LEA**
JONES DAY - ATLANTA GA
1221 PEACHTREE STREET NE
ATLANTA, GA 30361
404-581-8528
Fax: 404-581-8521
Email: blea@jonesday.com
ATTORNEY TO BE NOTICED

JAMES MAHONEY BURNHAM
DOJ-CIV

800 CONNECTICUT AVENUE NW
SUITE 300
WASHINGTON, DC 20006
602-501-5469
Email: james@kingstlegal.com
TERMINATED: 06/30/2023

Amicus**DEFI EDUCATION FUND**

represented by **BRIAN CHARLES LEA**
(See above for address)
ATTORNEY TO BE NOTICED

JAMES MAHONEY BURNHAM
(See above for address)
TERMINATED: 06/30/2023

Amicus**Bank Policy Institute**

represented by **JOHN KINCHEN**
SMYSER KAPLAN & VESELKA LLP -
HOUSTON TX
717 TEXAS AVENUE
SUITE 2800
HOUSTON, TX 77002
713-221-2345
Email: jkinchen@skv.com
ATTORNEY TO BE NOTICED

Date Filed	#	Select all / clear	Docket Text
10/12/2022	1	<input type="checkbox"/>	COMPLAINT against All Defendants (Filing fee \$ 402 receipt number AFLNDC-7505970.), filed by David Hoffman, Coin Center, John Doe, Patrick O'Sullivan. (Attachments: # 1 Civil Cover Sheet Civil Cover Sheet, # 2 Summons, # 3 Summons, # 4 Summons, # 5 Summons, # 6 Summons, # 7 Summons, # 8 Summons) (SASSO, MICHAEL) (Entered: 10/12/2022)
10/13/2022	2		DOCKET ANNOTATION BY COURT: The parties in the above-referenced case were added to the docket incorrectly and will be corrected by the clerk. Party names are to be entered in all caps and without punctuation. For future reference: Please review the procedure for adding/creating new parties in the "Style Guide for Electronic Case Filing" and/or chapter 10 of the "CM/ECF Attorney User's Guide," available at www.flnd.uscourts.gov. (mb) (Entered: 10/13/2022)
10/13/2022	3	<input type="checkbox"/>	Summons Issued as to JANET YELLEN (Attachments: # 1 DEPARTMENT OF THE TREASURY, # 2 ANDREA M GACKI, # 3 OFFICE OF FOREIGN ASSETS CONTROL). (mb) (Entered: 10/13/2022)
10/17/2022	4	<input type="checkbox"/>	Summons Issued as to U.S. Attorney General (Attachments: # 1 USA Civil Process Clerk, # 2 US ATTORNEY JASON COODY). (mb) (Entered: 10/17/2022)
11/06/2022	5	<input type="checkbox"/>	MOTION to Appear Pro Hac Vice by Jeffrey Hetzel.(Filing fee \$ 208 receipt number AFLNDC-7549344.) by COIN CENTER, JOHN DOE, DAVID

			HOFFMAN, PATRICK O'SULLIVAN. (Attachments: # 1 Exhibit Certificate of Good Standing) (HETZEL, JEFFREY) (Entered: 11/06/2022)
11/06/2022	6	<input type="checkbox"/>	MOTION to Appear Pro Hac Vice by Cameron T. Norris.(Filing fee \$ 208 receipt number AFLNDC-7549351.) by COIN CENTER, JOHN DOE, DAVID HOFFMAN, PATRICK O'SULLIVAN. (Attachments: # 1 Exhibit Certificate of Good Standing) (NORRIS, CAMERON) (Entered: 11/06/2022)
11/06/2022	7	<input type="checkbox"/>	MOTION to Appear Pro Hac Vice by Jeffrey Harris.(Filing fee \$ 208 receipt number AFLNDC-7549352.) by COIN CENTER, JOHN DOE, DAVID HOFFMAN, PATRICK O'SULLIVAN. (Attachments: # 1 Exhibit Certificate of Good Standing) (HARRIS, JEFFREY) (Entered: 11/06/2022)
11/07/2022			ACTION REQUIRED BY DISTRICT JUDGE: Chambers of JUDGE T KENT WETHERELL II notified that action is needed Re: 5 MOTION to Appear Pro Hac Vice by Jeffrey Hetzel.(Filing fee \$ 208 receipt number AFLNDC-7549344.), 6 MOTION to Appear Pro Hac Vice by Cameron T. Norris.(Filing fee \$ 208 receipt number AFLNDC-7549351.), 7 MOTION to Appear Pro Hac Vice by Jeffrey Harris.(Filing fee \$ 208 receipt number AFLNDC-7549352.) (mb) (Entered: 11/07/2022)
11/07/2022	8	<input type="checkbox"/>	ORDER granting 5 Motion to Appear Pro Hac Vice (Appointed JEFFREY HETZEL, CAMERON THOMAS NORRIS, JEFFREY MATTHEW HARRIS for COIN CENTER, PATRICK O'SULLIVAN, JOHN DOE, DAVID HOFFMAN); granting 6 Motion to Appear Pro Hac Vice (Appointed JEFFREY HETZEL, CAMERON THOMAS NORRIS, JEFFREY MATTHEW HARRIS for COIN CENTER, PATRICK O'SULLIVAN, JOHN DOE, DAVID HOFFMAN); granting 7 Motion to Appear Pro Hac Vice (Appointed JEFFREY HETZEL, CAMERON THOMAS NORRIS, JEFFREY MATTHEW HARRIS for COIN CENTER, PATRICK O'SULLIVAN, JOHN DOE, DAVID HOFFMAN). Signed by JUDGE T KENT WETHERELL II on 11/7/2022. (mb) (Entered: 11/07/2022)
12/08/2022	9	<input type="checkbox"/>	FIRST AMENDED COMPLAINT <i>with consent</i> against All Defendants All Defendants., filed by DAVID HOFFMAN, COIN CENTER, JOHN DOE, PATRICK O'SULLIVAN. (NORRIS, CAMERON) (Entered: 12/08/2022)
12/08/2022	10	<input type="checkbox"/>	CERTIFICATE OF SERVICE by COIN CENTER, JOHN DOE, DAVID HOFFMAN, PATRICK O'SULLIVAN re 9 Amended Complaint (NORRIS, CAMERON) (Entered: 12/08/2022)
12/16/2022	11	<input type="checkbox"/>	NOTICE of Appearance by CHRISTINE L COOGLE on behalf of All Defendants (COOGLE, CHRISTINE) (Entered: 12/16/2022)
12/16/2022	12	<input type="checkbox"/>	Consent MOTION for Extension of Time to File Answer by DEPARTMENT OF THE TREASURY, ANDREA M GACKI, OFFICE OF FOREIGN ASSETS CONTROL, JANET YELLEN. (Attachments: # 1 Text of Proposed Order) (COOGLE, CHRISTINE) (Entered: 12/16/2022)
12/19/2022	13	<input type="checkbox"/>	ORDER granting 12 Defendant's Unopposed MOTION for Extension of Time, and Defendants shall have until January 9, 2023, to answer or otherwise respond to the amended complaint. (Answer due by 1/9/2023 .) Signed by JUDGE T KENT WETHERELL II on 12/19/2022. (mb) (Entered: 12/19/2022)
01/04/2023	14	<input type="checkbox"/>	Joint MOTION for Discovery <i>Entry of Scheduling Order</i> by COIN CENTER, JOHN DOE, DAVID HOFFMAN, PATRICK O'SULLIVAN. (Attachments: # 1 Text of Proposed Order) (NORRIS, CAMERON) (Entered: 01/04/2023)

01/05/2023	15	<input type="checkbox"/>	INITIAL SCHEDULING ORDER re 14 Joint MOTION for Discovery <i>Entry of Scheduling Order</i> . Administrative Record. On or before 1/13/2023 , Defendants shall produce the certified administrative record to Plaintiffs and file a notice of service with the Court. The record itself shall not be filed with the Court until it becomes necessary for the Court to resolve any objections or consider the merits of the case. Objections. The parties shall meet and confer about any objections to the administrative record as soon as practicable after the record is served, and on or before 2/10/2023 , Plaintiffs shall file an appropriate motion raising any unresolved objections. Defendants shall have 14 days to respond to the objections. Proposed Briefing Schedule. If no objections to the administrative record are filed, the parties shall file a proposed summary judgment briefing schedule on or before 2/10/2023 . If objections are filed, the parties shall file the proposed briefing schedule within 7 days after the Court rules on the objections. Signed by JUDGE T KENT WETHERELL II on 1/5/2023. (mb) (Entered: 01/05/2023)
01/09/2023	16	<input type="checkbox"/>	ANSWER to 9 Amended Complaint by DEPARTMENT OF THE TREASURY, ANDREA M GACKI, OFFICE OF FOREIGN ASSETS CONTROL, JANET YELLEN. (COOGLE, CHRISTINE) (Entered: 01/09/2023)
01/09/2023	17	<input type="checkbox"/>	AMENDED ANSWER by DEPARTMENT OF THE TREASURY, ANDREA M GACKI, OFFICE OF FOREIGN ASSETS CONTROL, JANET YELLEN. Amendment to 16 Answer to Amended Complaint (<i>CORRECTED SIGNATURE BLOCK</i>). (COOGLE, CHRISTINE) (Entered: 01/09/2023)
01/10/2023	18	<input type="checkbox"/>	NOTICE of Appearance by CHRISTOPHER ROBERT HEALY on behalf of All Defendants (HEALY, CHRISTOPHER) (Entered: 01/10/2023)
01/13/2023	19	<input type="checkbox"/>	NOTICE of Service of Certified Administrative Record by DEPARTMENT OF THE TREASURY, ANDREA M GACKI, OFFICE OF FOREIGN ASSETS CONTROL, JANET YELLEN (Attachments: # 1 Certification, # 2 Index) (HEALY, CHRISTOPHER) (Entered: 01/13/2023)
02/08/2023	20	<input type="checkbox"/>	Joint MOTION to Extend Time by DEPARTMENT OF THE TREASURY, ANDREA M GACKI, OFFICE OF FOREIGN ASSETS CONTROL, JANET YELLEN. (HEALY, CHRISTOPHER) (Entered: 02/08/2023)
02/08/2023			ACTION REQUIRED BY DISTRICT JUDGE: Chambers of JUDGE T KENT WETHERELL II notified that action is needed Re: 20 JOINT MOTION TO AMEND THE SCHEDULE. (jff) (Entered: 02/08/2023)
02/09/2023	21	<input type="checkbox"/>	ORDER EXTENDING DEADLINES. Upon due consideration of the parties' joint motion to amend the schedule (Doc. 20), it is ORDERED that the motion is GRANTED, and the February 10, 2023, deadlines in the Initial Scheduling Order (Doc. 15) are extended to March 6, 2023. Signed by JUDGE T KENT WETHERELL II on 02/09/23. (Plaintiffs' motion or Parties' proposed briefing schedule deadline - 3/6/2023 .) (jff) (Entered: 02/09/2023)
02/28/2023	22	<input type="checkbox"/>	STIPULATION <i>Proposed Stipulated Protective Order</i> by DEPARTMENT OF THE TREASURY, ANDREA M GACKI, OFFICE OF FOREIGN ASSETS CONTROL, JANET YELLEN. (HEALY, CHRISTOPHER) (Entered: 02/28/2023)
03/01/2023	23	<input type="checkbox"/>	STIPULATED PROTECTIVE ORDER. (SEE FULL ORDER) Signed by JUDGE T KENT WETHERELL II on 03/01/23. (jff) (Entered: 03/01/2023)
03/06/2023	24	<input type="checkbox"/>	Joint MOTION Entry of Briefing Schedule by DEPARTMENT OF THE TREASURY, ANDREA M GACKI, OFFICE OF FOREIGN ASSETS

			CONTROL, JANET YELLEN. (HEALY, CHRISTOPHER) (Entered: 03/06/2023)
03/06/2023	25	<input type="checkbox"/>	MOTION for Protective Order <i>Precluding Extra-Record Expert Submission</i> by DEPARTMENT OF THE TREASURY, ANDREA M GACKI, OFFICE OF FOREIGN ASSETS CONTROL, JANET YELLEN. (Attachments: # 1 Text of Proposed Order) (HEALY, CHRISTOPHER) (Entered: 03/06/2023)
03/07/2023	26	<input type="checkbox"/>	ORDER ESTABLISHING BRIEFING SCHEDULE re 24 Parties' Joint MOTION for Entry of Briefing Schedule. That the Motion is GRANTED, and Plaintiffs' motion for summary judgment shall be filed or before May 12, 2023. Defendants' response and cross-motion for summary judgment shall be filed no later than 28 days after the motion is filed. Plaintiffs' reply and response to the cross-motion shall be filed no later than 21 days after the response/cross-motion is filed. Defendants reply shall be filed no later than 21 days after Plaintiffs' reply/response is filed. The joint appendix shall be filed no later than 7 days after the last brief is filed. (Motion for Summary Judgment due by 5/12/2023 ; Response to Motion and cross-motion due 6/9/2023 ; Replies due by 6/30/2023 ; Reply to reply/response 7/21/2023 ; Joint Appendix due by 7/28/2023). Signed by JUDGE T KENT WETHERELL II on 3/7/2023. (mb) (Entered: 03/07/2023)
03/07/2023	27	<input type="checkbox"/>	ORDER. Defendants' motion for a protective order (Doc. 25) is DENIED as premature. Signed by JUDGE T KENT WETHERELL II on 3/7/2023. (mb) (Entered: 03/07/2023)
03/14/2023	28	<input type="checkbox"/>	MOTION for Discovery to <i>Supplement Administrative Record with Expert Declaration</i> by COIN CENTER, JOHN DOE, DAVID HOFFMAN, PATRICK O'SULLIVAN. (Attachments: # 1 Exhibit Expert Declaration of Peter Van Valkenburgh, # 2 Exhibit Administrative Record Excerpts) (NORRIS, CAMERON) (Entered: 03/14/2023)
03/14/2023			Set Deadlines re 28 MOTION for Discovery to Supplement Administrative Record with Expert Declaration (Internal deadline for referral to judge if response not filed earlier: 3/28/2023). (mb) (Entered: 03/15/2023)
03/28/2023	29	<input type="checkbox"/>	MEMORANDUM in Opposition re 28 MOTION for Discovery to <i>Supplement Administrative Record with Expert Declaration</i> filed by DEPARTMENT OF THE TREASURY, ANDREA M GACKI, OFFICE OF FOREIGN ASSETS CONTROL, JANET YELLEN. (Attachments: # 1 Exhibit A - OFAC Evidentiary Memorandum, # 2 Exhibit B - Administrative Record Exhibit 62) (HEALY, CHRISTOPHER) (Entered: 03/28/2023)
03/28/2023			ACTION REQUIRED BY DISTRICT JUDGE: Chambers of JUDGE T KENT WETHERELL II notified that action is needed Re: 29 MEMORANDUM in Opposition re 28 MOTION for Discovery to Supplement Administrative Record with Expert Declaration filed by DEPARTMENT OF THE TREASURY, ANDREA M GACKI, OFFICE OF FOREIGN ASSETS CONTROL, JANET YELLEN. (Attachments: # 1 Exhibit A - OFAC Evidentiary Memorandum, # 2 Exhibit B - Administrative Record Exhibit 62). (mb) (Entered: 03/28/2023)
04/10/2023	30	<input type="checkbox"/>	ORDER DENYING MOTION TO SUPPLEMENT ADMINISTRATIVE RECORD. That Plaintiffs' motion to supplement the administrative record (Doc. 28) is DENIED. Signed by JUDGE T KENT WETHERELL II on 4/10/2023. (mb) (Entered: 04/10/2023)
04/28/2023	31	<input type="checkbox"/>	NOTICE of Errata re: <i>Truncated Exhibit</i> by DEPARTMENT OF THE TREASURY, ANDREA M GACKI, OFFICE OF FOREIGN ASSETS

			CONTROL, JANET FELLE (Attachments: # 1 Exhibit) (JANALY, CHRISTOPHER) (Entered: 04/28/2023)
04/28/2023	32	<input type="checkbox"/>	Consent MOTION for Extension of Time to File Dispositive Motions <i>Summary Judgment</i> by COIN CENTER, JOHN DOE, DAVID HOFFMAN, PATRICK O'SULLIVAN. (Attachments: # 1 Text of Proposed Order) (NORRIS, CAMERON) (Entered: 04/28/2023)
05/01/2023	33	<input type="checkbox"/>	ORDER re 32 Plaintiffs' Consent MOTION for Extension of Time. That the motion is GRANTED, and the deadline for Plaintiffs to file their motion for summary judgment is extended to May 26, 2023. (Motions due by 5/26/2023 .) Signed by JUDGE T KENT WETHERELL II on 5/1/2023. (mb) (Entered: 05/01/2023)
05/24/2023	34	<input type="checkbox"/>	MOTION to Appear Pro Hac Vice by Jessie K. Liu.(Filing fee \$ 208 receipt number AFLNDC-7885897.) by ANDREESSEN HOROWITZ. (Attachments: # 1 Exhibit Certificate of Good Standing) (LIU, JESSIE) (Entered: 05/24/2023)
05/25/2023	35	<input type="checkbox"/>	ORDER. This case is before the Court based on the motion for leave to appear pro hac vice filed by attorney Jessie K. Liu (Doc. 34). The motion is GRANTED, and attorney Jessie K. Liu is authorized to appear pro hac vice for potential amicus curiae Andreessen Horowitz. Signed by JUDGE T KENT WETHERELL II on 05/25/23. (jff) (Entered: 05/25/2023)
05/26/2023	36	<input type="checkbox"/>	MOTION for Summary Judgment by COIN CENTER, JOHN DOE, DAVID HOFFMAN, PATRICK O'SULLIVAN. (Internal deadline for referral to judge if response to summary judgment not filed earlier: 6/16/2023). (Attachments: # 1 Memorandum, # 2 Exhibit A (O'Sullivan Declaration), # 3 Exhibit B (Doe Declaration), # 4 Exhibit C (Hoffman Declaration), # 5 Exhibit D (Brito Declaration)) (NORRIS, CAMERON) (Entered: 05/26/2023)
05/31/2023	37	<input type="checkbox"/>	MOTION to Appear Pro Hac Vice by Alessio D. Evangelista.(Filing fee \$ 208 receipt number AFLNDC-7894791.) by ANDREESSEN HOROWITZ. (Attachments: # 1 Exhibit DC Certificate of Good Standing) (EVANGELISTA, ALESSIO) (Entered: 05/31/2023)
05/31/2023	38	<input type="checkbox"/>	MOTION to Appear Pro Hac Vice by Katherine C. Yarger.(Filing fee \$ 208 receipt number AFLNDC-7894777.) by Paradigm Operations LP. (Attachments: # 1 Certificate of Good Standing-Yarger) (YARGER, KATHERINE) (Entered: 05/31/2023)
05/31/2023			ACTION REQUIRED BY DISTRICT JUDGE: Chambers of JUDGE T KENT WETHERELL II notified that action is needed Re: 37 MOTION to Appear Pro Hac Vice by Alessio D. Evangelista, 38 MOTION to Appear Pro Hac Vice by Katherine C. Yarger. (mb) (Entered: 05/31/2023)
06/01/2023	39	<input type="checkbox"/>	ORDER re 38 MOTION to Appear Pro Hac Vice, 37 MOTION to Appear Pro Hac Vice. Attorney Alessio D. Evangelista is authorized to appear pro hac vice for potential amicus curiae Andreessen Horowitz. Attorney Katherine C. Yarger is authorized to appear pro hac vice for potential amicus curiae Paradigm Operations LP. Within 7 days from the date of this Order, the parties and potential amici shall confer and propose an amendment to the briefing schedule to establish deadlines for amicus briefs that ensures that the party whose position the amici oppose will have an opportunity to respond to the amici's arguments in the party's last brief. (Notify Chambers on 6/8/2023 .) Signed by JUDGE T KENT WETHERELL II on 6/1/2023. (mb) (Entered: 06/01/2023)

06/01/2023	40	<input type="checkbox"/>	MOTION to Appear Pro Hac Vice by James M. Burnham.(Filing fee \$ 208 receipt number AFLNDC-7898445.) by BLOCKCHAIN ASSOCIATION, DEFI EDUCATION FUND. (Attachments: # 1 Certificate of Good Standing) (BURNHAM, JAMES) (Entered: 06/01/2023)
06/02/2023			ACTION REQUIRED BY DISTRICT JUDGE: Chambers of JUDGE T KENT WETHERELL II notified that action is needed Re: 40 MOTION to Appear Pro Hac Vice by James M. Burnham.(Filing fee \$ 208 receipt number AFLNDC-7898445.) (mb) (Entered: 06/02/2023)
06/02/2023	41	<input type="checkbox"/>	ORDER re 40 Motion for Leave to Appear Pro Hac Vice. That the motion is GRANTED, and attorney James Burnham is authorized to appear pro hac vice for potential amicus curiae Blockchain Association and DeFi Education Fund. (Appointed JAMES MAHONEY BURNHAM for BLOCKCHAIN ASSOCIATION,JAMES MAHONEY BURNHAM for DEFI EDUCATION FUND). Signed by JUDGE T KENT WETHERELL II on 6/2/2023. (mb) (Entered: 06/02/2023)
06/02/2023	42	<input type="checkbox"/>	MOTION to File Amicus Brief <i>in Support of Plaintiffs' Motion for Summary Judgment</i> by BLOCKCHAIN ASSOCIATION, DEFI EDUCATION FUND. (Internal deadline for referral to judge if response not filed earlier: 6/16/2023). (Attachments: # 1 Exhibit A - Amicus Brief, # 2 Exhibit B - Text of Proposed Order) (LEA, BRIAN) (Entered: 06/02/2023)
06/02/2023	43	<input type="checkbox"/>	Joint MOTION to Extend Time <i>for Amendment of Scheduling Order to File Amicus Briefs</i> by BLOCKCHAIN ASSOCIATION, COIN CENTER, DEFI EDUCATION FUND, JOHN DOE, DAVID HOFFMAN, ANDREESSEN HOROWITZ, PATRICK O'SULLIVAN, Paradigm Operations LP. (Attachments: # 1 Text of Proposed Order) (NORRIS, CAMERON) (Entered: 06/02/2023)
06/02/2023	44	<input type="checkbox"/>	MOTION to Appear Pro Hac Vice by Rodrigo Seira.(Filing fee \$ 208 receipt number AFLNDC-7900903.) by Paradigm Operations LP. (Attachments: # 1 Certificate of Good Standing-Seira) (SEIRA, RODRIGO) (Entered: 06/02/2023)
06/02/2023	45	<input type="checkbox"/>	MOTION for Leave to File <i>Amicus Brief on Behalf of Paradigm Operations LP in Support of Plaintiffs' Motion for Summary Judgment</i> by Paradigm Operations LP. (Attachments: # 1 Exhibit A - Brief of Amicus Curiae Paradigm Operations LP In Support of Plaintiffs' Motion for Summary Judgment, # 2 Exhibit B - [Proposed] Order Granting Unopposed Motion for Leave to File Amicus Brief) (YARGER, KATHERINE) (Entered: 06/02/2023)
06/02/2023	46	<input type="checkbox"/>	MOTION to File Amicus Brief <i>in Support of Plaintiffs' Motion for Summary Judgment</i> by ANDREESSEN HOROWITZ. (Internal deadline for referral to judge if response not filed earlier: 6/16/2023). (Attachments: # 1 Exhibit A - Brief of Andreessen Horowitz as Amicus Curiae in Support of Plaintiffs' Motion for Summary Judgment, # 2 Exhibit B - [Proposed] Order Granting Motion for Leave to File Amicus Brief on Behalf of Andreessen Horowitz as Amicus Curiae in Support of Plaintiffs' Motion for Summary Judgment) (EVANGELISTA, ALESSIO) (Entered: 06/02/2023)
06/05/2023			ACTION REQUIRED BY DISTRICT JUDGE: Chambers of JUDGE T KENT WETHERELL II notified that action is needed Re: 43 Joint MOTION to Extend Time <i>for Amendment of Scheduling Order to File Amicus Briefs</i> , 44 MOTION to Appear Pro Hac Vice by Rodrigo Seira, 45 MOTION for Leave to File <i>Amicus Brief on Behalf of Paradigm Operations LP in Support of Plaintiffs' Motion for Summary Judgment</i> . (mb) (Entered: 06/05/2023)

06/05/2023	47	<input type="checkbox"/>	ORDER ACCEPTING AMICUS BRIEFS. That the motions are GRANTED, and the amicus briefs (Docs. 42 -1, 45 -1, 46 -1) are accepted and deemed filed. Signed by JUDGE T KENT WETHERELL II on 6/5/2023. (mb) (Entered: 06/05/2023)
06/05/2023	48	<input type="checkbox"/>	ORDER re 44 MOTION for Leave to appear Pro Hac Vice. That the motion is GRANTED, and attorney Rodrigo Seira is authorized to appear pro hac vice for amicus curiae Paradigm Operations LP. (Appointed RODRIGO SEIRA for Paradigm Operations LP). Signed by JUDGE T KENT WETHERELL II on 6/5/2023. (mb) (Entered: 06/05/2023)
06/05/2023	49	<input type="checkbox"/>	ORDER SUPPLEMENTING BRIEFING SCHEDULE re 43 Parties' Joint MOTION for Amendment of Scheduling Order. Amicus briefs in support of Plaintiffs shall be filed on or before 6/2/2023 . Amicus briefs in support of Defendants shall be filed on or before 6/30/2023 . Signed by JUDGE T KENT WETHERELL II on 6/5/2023. (mb) (Entered: 06/05/2023)
06/12/2023	50	<input type="checkbox"/>	First MOTION to Appear Pro Hac Vice by Eric Tung.(Filing fee \$ 208 receipt number AFLNDC-7915765.) by BLOCKCHAIN ASSOCIATION, DEFI EDUCATION FUND. (Attachments: # 1 Certificate of Good Standing) (TUNG, ERIC) (Entered: 06/12/2023)
06/13/2023			ACTION REQUIRED BY DISTRICT JUDGE: Chambers of JUDGE T KENT WETHERELL II notified that action is needed Re: 50 First MOTION to Appear Pro Hac Vice by Eric Tung.(Filing fee \$ 208 receipt number AFLNDC-7915765.) (mb) (Entered: 06/13/2023)
06/13/2023	51	<input type="checkbox"/>	ORDER re 50 Motion to Appear Pro Hac Vice. That the motion is GRANTED, and attorney Eric Tung is authorized to appear pro hac vice for amici Blockchain Association and DeFi Education Fund. Signed by JUDGE T KENT WETHERELL II on 6/12/2023. (mb) (Entered: 06/13/2023)
06/15/2023	52	<input type="checkbox"/>	Consent MOTION to Extend Time by DEPARTMENT OF THE TREASURY, ANDREA M GACKI, OFFICE OF FOREIGN ASSETS CONTROL, JANET YELLEN. (Attachments: # 1 Text of Proposed Order) (COOGLE, CHRISTINE) (Entered: 06/15/2023)
06/15/2023			ACTION REQUIRED BY DISTRICT JUDGE: Chambers of JUDGE T KENT WETHERELL II notified that action is needed Re: 52 Consent MOTION to Extend Time. (mb) (Entered: 06/15/2023)
06/15/2023	53	<input type="checkbox"/>	NOTICE of Errata by DEPARTMENT OF THE TREASURY, ANDREA M GACKI, OFFICE OF FOREIGN ASSETS CONTROL, JANET YELLEN re 52 Consent MOTION to Extend Time (Attachments: # 1 Corrected Motion, # 2 Text of Proposed Order) (COOGLE, CHRISTINE) (Entered: 06/15/2023)
06/15/2023			ACTION REQUIRED BY DISTRICT JUDGE: Chambers of JUDGE T KENT WETHERELL II notified that action is needed Re: 53 Notice OF Errata. (jff) (Entered: 06/15/2023)
06/16/2023	54	<input type="checkbox"/>	ORDER GRANTING EXTENSION OF TIME. Upon due consideration of Defendants' corrected consent motion for extension of time (Doc. 53 -1), it is ORDERED that the motion is GRANTED, and the deadline for Defendants' response/cross-motion for summary judgment is extended to June 30, 2023. Signed by JUDGE T KENT WETHERELL II on 06/16/23. (Internal deadline for referral to judge if response not filed earlier: 6/30/2023 .) (jff) (Entered: 06/16/2023)

06/29/2023	55	<input type="checkbox"/>	MOTION to Withdraw as Attorney <i>James Burnham</i> by BLOCKCHAIN ASSOCIATION, DEFI EDUCATION FUND. (BURNHAM, JAMES) (Entered: 06/29/2023)
06/29/2023			Set Deadlines re 55 MOTION to Withdraw as Attorney (Internal deadline for referral to judge if response not filed earlier: 7/13/2023). (mb) (Entered: 06/30/2023)
06/30/2023	56	<input type="checkbox"/>	ORDER re 55 Motion to Withdraw as Attorney. That the motion is GRANTED, and James M. Burnham shall have no further obligation to represent the Blockchain Association and DeFi Education Fund in this case. The Clerk shall terminate Mr. Burnham as counsel of record in CM/ECF. Attorney JAMES MAHONEY BURNHAM terminated. Signed by JUDGE T KENT WETHERELL II on 6/30/2023. (mb) (Entered: 06/30/2023)
06/30/2023	57	<input type="checkbox"/>	MEMORANDUM in Opposition re 36 MOTION for Summary Judgment <i>and Cross-Motion for Summary Judgment</i> filed by DEPARTMENT OF THE TREASURY, ANDREA M GACKI, OFFICE OF FOREIGN ASSETS CONTROL, JANET YELLEN. (Attachments: # 1 Exhibit A) (COOGLE, CHRISTINE) (Entered: 06/30/2023)
06/30/2023			Set Deadlines re 57 MEMORANDUM in Opposition re 36 MOTION for Summary Judgment and Cross-Motion for Summary Judgment. (Replies due by 7/21/2023). (mb) (Entered: 07/03/2023)
07/06/2023	58	<input type="checkbox"/>	MOTION to Appear Pro Hac Vice by John Kinchen.(Filing fee \$ 208 receipt number AFLNDC-7952539.) by Bank Policy Institute. (Attachments: # 1 Exhibit Certificate of Good Standing) (KINCHEN, JOHN) (Entered: 07/06/2023)
07/06/2023			ACTION REQUIRED BY DISTRICT JUDGE: Chambers of JUDGE T KENT WETHERELL II notified that action is needed Re: 58 MOTION to Appear Pro Hac Vice by John Kinchen. (Filing fee \$ 208 receipt number AFLNDC-7952539.) (mb) (Entered: 07/06/2023)
07/07/2023	59	<input type="checkbox"/>	ORDER RE 58 Motion to Appear Pro Hac Vice. That the motion is GRANTED, and attorney John Kinchen is authorized to appear pro hac vice for potential amicus curiae Bank Policy Institute. (Appointed JOHN KINCHEN for Bank Policy Institute). Signed by JUDGE T KENT WETHERELL II on 7/7/2023. (mb) (Entered: 07/07/2023)
07/07/2023	60	<input type="checkbox"/>	MOTION for Leave to File <i>Amicus Brief on Behalf of The Bank Policy Institute in Support of Defendants' Cross-Motion for Summary Judgment</i> by Bank Policy Institute. (Attachments: # 1 Exhibit Brief of Amicus Curiae The Bank Policy Institute, # 2 Exhibit Proposed Order Granting Motion for Leave) (KINCHEN, JOHN) (Entered: 07/07/2023)
07/10/2023			ACTION REQUIRED BY DISTRICT JUDGE: Chambers of JUDGE T KENT WETHERELL II notified that action is needed Re: 60 MOTION for Leave to File <i>Amicus Brief on Behalf of The Bank Policy Institute in Support of Defendants' Cross-Motion for Summary Judgment</i> (mb) (Entered: 07/10/2023)
07/10/2023	61	<input type="checkbox"/>	ORDER re 60 BANK POLICY INSTITUTE's Unopposed Motion to File Amicus Brief. That the motion is GRANTED, and the Bank Policy Institute's amicus brief (Doc. 60 -1) is accepted. Signed by JUDGE T KENT WETHERELL II on 7/10/2023. (mb) (Entered: 07/10/2023)
07/21/2023	62	<input type="checkbox"/>	MEMORANDUM in Opposition re 36 MOTION for Summary Judgment , REPLY to Response to Motion filed by COIN CENTER, JOHN DOE, DAVID

USCA11 Case: 23-13688 Document 14-1 Date Filed: 10/18/23 Page 20 of 243			
			HOFFMAN, PATRICK O'SULLIVAN, (NORRIS, CAMERON) (Entered: 07/21/2023)
07/21/2023			Set Deadlines re 62 MEMORANDUM in Opposition re 36 MOTION for Summary Judgment, REPLY to Response to Motion. (Replies due by 7/31/2023). (mb) (Entered: 07/24/2023)
07/31/2023	63	<input type="checkbox"/>	Consent MOTION for Extension of Word Limit by DEPARTMENT OF THE TREASURY, ANDREA M GACKI, OFFICE OF FOREIGN ASSETS CONTROL, JANET YELLEN. (Attachments: # 1 Text of Proposed Order) (COOGLE, CHRISTINE) (Entered: 07/31/2023)
08/01/2023			ACTION REQUIRED BY DISTRICT JUDGE: Chambers of JUDGE T KENT WETHERELL II notified that action is needed Re: 63 Consent MOTION for Extension of Word Limit (mb) (Entered: 08/01/2023)
08/01/2023	64	<input type="checkbox"/>	ORDER INCREASING WORD LIMIT re 63 Defendants' Consent MOTION for Extension of Word Limit. That the motion is GRANTED, and Defendants' reply may be up to 6,000 words in length. Signed by JUDGE T KENT WETHERELL II on 8/1/2023. (mb) (Entered: 08/01/2023)
08/03/2023	65	<input type="checkbox"/>	ORDER re 15 Order and 26 ORDER ESTABLISHING BRIEFING SCHEDULE. That the parties shall provide a hard copy of the administrative record / joint appendix to the Court contemporaneously with the filing of the electronic copy filed through CM/ECF. (Notify Chambers on 8/10/2023 if document not filed.) Signed by JUDGE T KENT WETHERELL II on 8/3/2023. (mb) (Entered: 08/03/2023)
08/11/2023			ACTION REQUIRED BY DISTRICT JUDGE: Chambers of JUDGE T KENT WETHERELL II notified that action is needed Re: 65 Order. (Documents not filed, nor hard copies received). (mb) (Entered: 08/11/2023)
08/11/2023	66	<input type="checkbox"/>	Defendant's REPLY to Response to Motion re 36 MOTION for Summary Judgment and 57 MEMORANDUM in Opposition and Cross-Motion for Summary Judgment filed by DEPARTMENT OF THE TREASURY, ANDREA M GACKI, OFFICE OF FOREIGN ASSETS CONTROL, JANET YELLEN. (COOGLE, CHRISTINE) (Entered: 08/11/2023)
08/14/2023			ACTION REQUIRED BY DISTRICT JUDGE: Chambers of JUDGE T KENT WETHERELL II notified that action is needed Re: 66 Defendant's REPLY to Response to Motion re 36 MOTION for Summary Judgment and 57 MEMORANDUM in Opposition and Cross-Motion for Summary Judgment filed by DEPARTMENT OF THE TREASURY, ANDREA M GACKI, OFFICE OF FOREIGN ASSETS CONTROL, JANET YELLEN. (mb) (Entered: 08/14/2023)
08/18/2023	67	<input type="checkbox"/>	NOTICE of JOINT APPENDIX of Administrative Record Documents Cited in Parties' Cross-Motions for Summary Judgment, by COIN CENTER, JOHN DOE, DAVID HOFFMAN, PATRICK O'SULLIVAN re 57 Memorandum in Opposition to 36 MOTION for Summary Judgment, filed by CAMERON T NORRIS, counsel for Plaintiffs. (JOINT APPENDIX Volume 1 and JOINT APPENDIX Volume 2 received). (mb) (Entered: 08/18/2023)
08/18/2023	68	<input type="checkbox"/>	NOTICE by COIN CENTER, JOHN DOE, DAVID HOFFMAN, PATRICK O'SULLIVAN re 57 Memorandum in Opposition to Motion, 66 Reply to Response to Motion, 36 MOTION for Summary Judgment , 62 Memorandum in Opposition to Motion, Reply to Response to Motion (Attachments: # 1 Appendix Joint Appendix Vol. I, # 2 Appendix Joint Appendix Vol. II) (NORRIS, CAMERON) (Entered: 08/18/2023)

08/18/2023	69	<input type="checkbox"/>	NOTICE of Classified Lodging by DEPARTMENT OF THE TREASURY, ANDREA M GACKI, OFFICE OF FOREIGN ASSETS CONTROL, JANET YELLEN (COOGLE, CHRISTINE) (Entered: 08/18/2023)
08/18/2023	70	<input type="checkbox"/>	NOTICE of Supplemental Authority by DEPARTMENT OF THE TREASURY, ANDREA M GACKI, OFFICE OF FOREIGN ASSETS CONTROL, JANET YELLEN (Attachments: # 1 Exhibit) (COOGLE, CHRISTINE) (Entered: 08/18/2023)
08/21/2023	71	<input type="checkbox"/>	RESPONSE by COIN CENTER, JOHN DOE, DAVID HOFFMAN, PATRICK O'SULLIVAN re 70 Notice (Other) of Supplemental Authority. (NORRIS, CAMERON) (Entered: 08/21/2023)
08/21/2023			ACTION REQUIRED BY DISTRICT JUDGE: Chambers of JUDGE T KENT WETHERELL II notified that action is needed Re: 71 RESPONSE by COIN CENTER, JOHN DOE, DAVID HOFFMAN, PATRICK O'SULLIVAN re 70 Notice (Other) of Supplemental Authority. (mb) (Entered: 08/21/2023)
08/22/2023	72	<input type="checkbox"/>	MOTION for Leave to File re 70 Notice (Other), 71 Response/Reply <i>Reply</i> by DEPARTMENT OF THE TREASURY, ANDREA M GACKI, OFFICE OF FOREIGN ASSETS CONTROL, JANET YELLEN. (COOGLE, CHRISTINE) (Entered: 08/22/2023)
08/22/2023			Set Deadlines re 72 MOTION for Leave to File Document. (Internal deadline for referral to judge if response not filed earlier: 9/5/2023). (mb) (Entered: 08/23/2023)
08/23/2023	73	<input type="checkbox"/>	ORDER DENYING LEAVE TO FILE REPLY. Defendants' motion for leave to file a reply (Doc. 72) is DENIED. Signed by JUDGE T KENT WETHERELL II on 8/23/2023. (mb) (Entered: 08/23/2023)
10/30/2023	74	<input type="checkbox"/>	ORDER ON CROSS-MOTIONS FOR SUMMARY JUDGMENT. Plaintiffs' motion for summary judgment (Doc. 36) is DENIED. Defendants' cross-motion for summary judgment (Doc. 57) is GRANTED. The Clerk shall enter judgment stating: "Summary judgment is entered in favor of Defendants. All claims in Plaintiffs' amended complaint are dismissed with prejudice. Plaintiffs shall take nothing from this action and Defendants shall go hence without delay." The Clerk shall close the case file. Signed by JUDGE T KENT WETHERELL II on 10/30/2023. (mb) (Entered: 10/30/2023)
10/30/2023	75	<input type="checkbox"/>	CLERK'S JUDGMENT re 74 ORDER ON CROSS-MOTIONS FOR SUMMARY JUDGMENT. (mb) (Entered: 10/30/2023)
11/06/2023	76	<input type="checkbox"/>	NOTICE OF APPEAL as to 75 Clerk's Judgment by COIN CENTER, JOHN DOE, DAVID HOFFMAN, PATRICK O'SULLIVAN. (Filing fee \$505 Receipt Number AFLNDC-8359001.) (NORRIS, CAMERON) (Entered: 11/06/2023)
11/07/2023	77		Appeal Instructions re: 76 Notice of Appeal : The Transcript Request Form is available on the Internet at https://www.flnd.uscourts.gov/form/eleventh-circuit-transcript-information-form **PLEASE NOTE** Separate forms must be filed for each court reporter in both the district court and the appeals court. Transcript Order Form due by 11/21/2023 . (mb) (Entered: 11/07/2023)
11/07/2023	78	<input type="checkbox"/>	Transmission of Notice of Appeal and Docket Sheet to US Court of Appeals re 76 Notice of Appeal. (mb) (Entered: 11/07/2023)

11/08/2023	79	<input type="checkbox"/>	USCA PROCEDURAL LETTER re: 76 NOTICE OF APPEAL as to 75 Clerk's Judgment by COIN CENTER, JOHN DOE, DAVID HOFFMAN, PATRICK O'SULLIVAN. CIVIL APPEAL DOCKETED. USCA Appeal # 23-13698-E (jff) (Entered: 11/13/2023)
11/15/2023	80	<input type="checkbox"/>	TRANSCRIPT REQUEST by COIN CENTER, JOHN DOE, DAVID HOFFMAN, PATRICK O'SULLIVAN for proceedings held on (no transcripts ordered) before Judge (no transcripts ordered), (NORRIS, CAMERON) (Entered: 11/15/2023)

[View Selected](#)

or

[Download Selected](#)

PACER Service Center			
Transaction Receipt			
12/08/2023 11:34:00			
PACER Login:	bg0034bg	Client Code:	
Description:	Docket Report	Search Criteria:	3:22-cv-20375-TKW-ZCB
Billable Pages:	13	Cost:	1.30

TAB 9

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF FLORIDA
PENSACOLA DIVISION**

COIN CENTER; PATRICK
O’SULLIVAN; JOHN DOE; and
DAVID HOFFMAN,

Plaintiffs,

v.

JANET YELLEN, in her official
capacity as Secretary of the Treasury;
DEPARTMENT OF THE
TREASURY; ANDREA M. GACKI,
in her official capacity as Director of
the Office of Foreign Assets Control;
and OFFICE OF FOREIGN
ASSETS CONTROL,

Defendants.

Case No.

3:22-cv-20375-TKW-ZCB

FIRST AMENDED COMPLAINT

Plaintiffs file this complaint for declaratory and injunctive relief against Defendants and allege as follows.

NATURE OF THE ACTION

1. On August 8, 2022, and then again on November 8, 2022, the Biden Administration criminalized an open-source software tool that helps Americans maintain their privacy while using cryptocurrency and related assets. It justified this action based on its power to sanction foreign enemies, even though the tool is not

controlled by foreign enemies and Americans' use of the tool does not involve foreign enemies. The Administration's invocation of the foreign-affairs power to punish domestic cryptocurrency users was unprecedented and unlawful.

2. Plaintiffs all use Ethereum. Ethereum is a digital marketplace that uses shared online technology to help people order their finances without needing to trust banks, governments, or other third parties. It enables transactions involving cryptocurrency and other similar crypto assets. Tens of millions of Americans use Ethereum.

3. Ethereum's functionality depends on a transparent public ledger. When someone completes a transaction using Ethereum, that transaction is posted to a ledger visible to anyone. The transaction can't be erased or hidden from view. Although users transact using pseudonymous addresses, there are a variety of ways to connect a person's identity to his address on the public ledger—and therefore to all his transactions and assets.

4. If a user doesn't take proactive steps to protect his privacy, the ledger's transparency allows strangers to track his private associations and stalk his intimate relations. It invites publicization of and retaliation for his private contributions to unpopular causes. And it allows anyone to see whether he has a lot of assets, which can put a target on his back.

5. To protect themselves, users of Ethereum employ privacy tools. These tools generally allow users to clear any publicly discernible connection between their

past and future transactions. They do this by making transactions by the same person appear unrelated, thereby stymying bad actors who seek to track, stalk, retaliate, and endanger.

6. The state-of-the-art privacy tool on Ethereum is the Tornado Cash Tool. The Tornado Cash Tool is a software program permanently stored on the Ethereum ledger, so it can be accessed or used by anyone. To use the Tornado Cash Tool, a user moves his crypto assets to a Tornado Cash Tool address. There are several such addresses, each for a different type of crypto asset or a different amount of that asset. After moving his asset to that address, the user can then direct the asset's release to a new address, controlled either by him or by his chosen recipient.

7. To anyone viewing the public ledger, it is impossible to tell when the person retrieved his asset or which new address it went to. Once the asset arrives at the new address, it cannot be connected to the earlier address using publicly available data. If the user wishes to relink the two addresses and prove that both were his, he can do so, selectively revealing his identity, but no stranger can perform this re-identification without his consent.

8. Nobody controls the Tornado Cash Tool. It is immutable and executes according to the user's wishes. The Tool is software residing on the Ethereum public ledger at specified Ethereum addresses. Anyone with an internet connection can move crypto assets to those addresses and make the software perform the aforementioned

steps to protect that user's privacy. Throughout this entire process no human or organization, apart from the user, can or does hold the assets.

9. Cryptocurrencies like Bitcoin are known, in part, for creating irreversible transactions that, once confirmed in the shared public ledger online, cannot be canceled, withdrawn, altered, or rescinded by the sender or any third party. This quality is often referred to as immutability. Ethereum takes this capability a step further and allows technologists to publish immutable software tools to the public ledger. Once published, these tools are available for anyone with an internet connection to use, and they will perform exactly as the rules in their software command. No person or organization can alter their functionality or remove their availability, just as no person or organization can reverse or rescind a cryptocurrency payment.

10. The people who wrote the Tornado Cash Tool can use the Tool just like anyone else. But because the Tool is published to the public ledger in an immutable form, those people no longer have any say in who uses the Tool or any involvement in Americans' use of the Tool. Likewise, a decentralized autonomous organization exists with regard to some similar non-immutable software, but that organization has no power over the Tornado Cash Tool.

11. The International Emergency Economic Powers Act of 1977, which is the statutory descendant of the Trading with the Enemy Act of 1917, allows the President to restrict trade with foreign enemies under emergency conditions.

12. As relevant here, it authorizes the President to “declar[e] a national emergency with respect to” an “unusual and extraordinary” foreign threat. 50 U.S.C. §1701(a).

13. Once the President declares that emergency, the Act allows him to criminalize certain transactions, but only if the transactions are “in foreign exchange” or include “any property in which any foreign country or a national thereof has any interest.” *Id.* §1702(a)(1).

14. The North Korea Sanctions and Policy Enhancement Act gives the President specific authority to criminalize transactions with North Korean-related persons within the same scope. 22 U.S.C. §§9201 et seq. For instance, he can criminalize transactions involving qualifying North-Korean-related “person[s]” when those transactions are “in foreign exchange.” 22 U.S.C. §9214; *see also, e.g., id.* §§9214(c), 9214(f), §9221c.

15. Under executive delegations and regulations, Defendants exercise a subpart of the President’s power under these Acts. Specifically, under certain conditions, Defendants can criminalize transactions that fall within the scope of the Acts, but only by designating “persons” or “entities” with whom Americans cannot trade. 31 C.F.R. §578.201(a), §510.201(a).

16. Invoking this authority last August, Defendants criminalized all transactions involving 38 Ethereum addresses. Those 38 addresses included 20 addresses at which the Tornado Cash Tool is published.

17. In November, after this lawsuit was originally filed, Defendants withdrew that action. But on the same day, Defendants criminalized all transactions involving a batch of 90 Ethereum addresses, including 29 addresses at which the Tornado Cash Tool is published. Those 29 addresses constitute the core of the Tornado Cash Tool.

18. The criminalization of those 29 addresses is at issue in this lawsuit.

19. In their second attempt to criminalize the Tornado Cash Tool, Defendants altered their justification for their action. But they did not invoke any broader authority relevant to Plaintiffs' claims.

20. Defendants also put into the daylight their confused view of what they were criminalizing. Recognizing that they can criminalize transactions only if those transactions involve qualifying foreign “person[s]” and “entit[ies],” Defendants identified the “founders and other associated developers” of the software underlying the Tool, as well as a decentralized autonomous organization that has no control over the Tool, as together constituting an entity that Defendants called “the Tornado Cash person.” *See Frequently Asked Questions No. 1095*, Dep’t of Treasury, perma.cc/VT4V-T7JJ (“Who is the Tornado Cash “person” that OFAC designated[?]”). They then reasoned that these people and this organization “*use*” the Tornado Cash Tool to further a broad range of goals. *Id.* (emphasis added). But, then, instead of criminalizing transactions with the people and organization themselves, as

the governing law allows, Defendants criminalized transactions with the Tornado Cash Tool that they use. *Id.*

21. In other words, Defendants’ new action identifies people and an organization whom they *could* sanction, explains that those people and that organization “use” a technology, and then proceeds to sanction the technology but not the people or the organization.

22. As a result, an American today could send cryptocurrency directly to those sanctionable people and organizations without repercussion. But if that same American used the Tornado Cash Tool to move his own cryptocurrency to his own new address in a process entirely beyond the control of any of these people or organizations, he would commit a federal crime.

23. Americans who use the Tornado Cash Tool to protect their privacy while using their own assets or while transacting with each other are now criminals. Their receipt of any asset through the Tornado Cash Tool, even one that they did not solicit, is a federal crime. And their use of the Tornado Cash Tool to protect their expressive activities is criminal as well.

24. Defendants’ action was unlawful for four main reasons.

25. First, Defendants’ criminalization of the Tornado Cash Tool exceeded their statutory authority because the Tornado Cash Tool is used to complete functions that do not involve qualifying “person[s],” are not “in foreign exchange,” and do not include “any property in which any foreign country or a national thereof has any

interest.” 50 U.S.C. §1702(a)(1); 22 U.S.C. §§9201 et seq. Americans use the Tornado Cash Tool unilaterally to protect their own property. Defendants’ defiance of this statutory element assumes an authority that would give them virtually unlimited control to regulate the American economy.

26. Second, Defendants’ criminalization of the Tornado Cash Tool also exceeded their regulatory authority because the Tornado Cash Tool is not a “person.” 31 C.F.R. §§578.201(a), §510.201(a). It is a privacy tool beyond the control of anyone.

27. Third, Defendants’ criminalization of the Tornado Cash Tool was arbitrary and capricious because it failed to consider important aspects of the problem, changed their position without explanation, was pretextual, and defied their own rules on the books.

28. And fourth, Defendants’ criminalization of the Tornado Cash Tool violated the constitutional rights of users of the Tornado Cash Tool who need it to protect their private associations.

29. Plaintiffs all would have used or continued to use the Tornado Cash Tool to protect their privacy in the future, but are prevented from doing so as a result of the Biden Administration’s criminalization of the Tornado Cash Tool.

30. They respectfully request that this Court hold unlawful, set aside, and permanently enjoin the enforcement of the criminalization of the Tornado Cash Tool.

THE PARTIES

31. Plaintiff Coin Center is the leading nonprofit research and advocacy center focused on the public-policy issues facing cryptocurrency and decentralized computing technologies. It defends the rights of individuals to build and use free and open cryptocurrency networks, including the right to write and publish code, the right to assemble into peer-to-peer networks, and the right to do all this privately. Coin Center produces and publishes research, educates policymakers and the media about cryptocurrencies, advocates for sound public policy, and defends digital civil liberties. It is based in Washington, D.C.

32. Coin Center uses Ethereum. It routinely receives contributions from donors in the form of crypto assets.

33. Many of Coin Center's donors want to keep their contributions private. They value privacy, both when it comes to public knowledge of their crypto assets and public knowledge of their expressive associations. Many of them engage in transactions that can be traced on Ethereum's public ledger with the assets that they intend to contribute to Coin Center.

34. Coin Center's donors therefore used in the past, and would use in the future, the Tornado Cash Tool to protect their privacy. They would send a crypto asset to a Tornado Cash Tool address, and then release it to an address controlled by Coin Center. It is impossible to tell whose assets are being sent to Coin Center's account when they come from a Tornado Cash Tool address.

35. As a result of the Biden Administration's criminalization of the Tornado Cash Tool, these donors are less likely to contribute to Coin Center. They are effectively barred from engaging in expressive advocacy because, without the Tornado Cash Tool, they cannot do so with confidence that their associations will remain private. By forcing them to make contributions on the public ledger, the Biden Administration's criminalization of the Tornado Cash Tool chills their expressive activity. Coin Center will lose contributions from these donors.

36. Coin Center is not a terrorist or a criminal and does not intend to transact with terrorists or criminals. In the course of receiving contributions through the Tornado Cash Tool from American donors, the donors' and Coin Center's assets would never come under the control of any foreign person or organization.

37. Plaintiff Patrick O'Sullivan is a software developer who resides in Escambia County, Florida.

38. Mr. O'Sullivan uses Ethereum. He is routinely paid by his employer in crypto assets, and he routinely obtains crypto assets from public exchanges.

39. Mr. O'Sullivan's use of Ethereum can be monitored on Ethereum's public ledger. Mr. O'Sullivan shares his Ethereum addresses with other parties, transfers assets to himself from accounts with third parties who hold his personal information, and is a publicly known user and developer of Ethereum-related technology. As a result, Mr. O'Sullivan's transactions and assets can easily be tracked by the public at large.

40. He therefore routinely uses privacy tools to protect himself and his family. He has used a number of privacy tools, each of which has its own advantages.

41. Mr. O'Sullivan believes that the best practice for protecting his privacy is to use multiple privacy tools. Mr. O'Sullivan believes that the Tornado Cash Tool is one of the best options for protecting his privacy. And Mr. O'Sullivan does not believe that alternatives, standing alone, would provide him with adequate privacy and security. He therefore intended to use the Tornado Cash Tool in his regular rotation of privacy tools.

42. Mr. O'Sullivan intended to move assets from an address under his control to a Tornado Cash Tool address and then later release them to a new address, also under his control. At no point would these assets have been controlled by anyone else, including any person or organization.

43. All of Mr. O'Sullivan's crypto assets come from his American employer or from public exchanges. He is not a terrorist or a criminal and does not intend to transact with terrorists or criminals. In using Tornado Cash, his assets would never come under the control of any other person or organization, including any foreign person or organization.

44. As a result of Defendants' action, Mr. O'Sullivan cannot carry out his intended uses of the Tornado Cash Tool.

45. John Doe is a human-rights advocate who resides in the southeastern United States. Mr. Doe is proceeding anonymously because he credibly fears that, if

his identity is exposed, Russian agents will learn about his pro-Ukrainian activities and will harm him and his family.

46. After Russia invaded Ukraine, Mr. Doe began providing and coordinating support for Ukrainians under attack. Since April 2022, he has been supporting Ukrainians personally and has facilitated sizable crypto donations from other donors. He and his donors call themselves the 688th Support Brigade.

47. Mr. Doe provides and facilitates donations that go to supporting the most urgent needs of Ukrainians at war. His efforts have paid for gloves, shoes, helmets, drones, and vehicles to assist Ukrainian frontline efforts. While many say they support Ukraine, Mr. Doe and his donors are actually doing something about it.

48. Crypto donations to Ukraine have made a substantial positive impact. As Senator Toomey recently recounted in a congressional hearing, “While there has been virtually no evidence of Russia meaningfully using cryptocurrencies to evade sanctions, Ukraine has been actively utilizing cryptocurrencies to do tremendous good. Cryptocurrency donations for Ukraine have reached approximately \$100 million, which has helped Ukrainians defend their country against Russia’s invasion. These funds have gone towards more than 5,500 bulletproof vests, 500 helmets, and 410,000 meals, among other things. Ukraine’s Deputy Minister of Digital Transformation has said that ‘each and every helmet and vest bought via crypto donations is currently saving Ukrainian soldiers’ lives.’”

49. Mr. Doe and the donors he assists came to the mutual agreement that donating to Ukrainians could jeopardize their and their families' safety. Without privacy protections, Russian agents and Russian-funded hackers could identify and retaliate against donors for providing frontline aid. If the donors' identities were revealed, their lives could be in danger when they travel abroad and they could be targeted by hackers. Mr. Doe's donors want to support Ukraine without fear of being harmed. They also inherently value making contributions privately.

50. Every single donor has used the Tornado Cash Tool. Under Mr. Doe's direction, a donor will move his crypto asset to a Tornado Cash Tool address, then later release it from that address to an account controlled by Mr. Doe exclusively for the provision of aid. From that latter account, Mr. Doe can send the assets to recipients who purchase the aid for Ukraine. It is impossible for an outside observer to tell whose assets are being sent to the latter account because they all come through an address with this privacy tool.

51. Mr. Doe himself has contributed to these efforts using the Tornado Cash Tool. He has moved assets from a personal address to a Tornado Cash Tool address, and then released those assets from the Tornado Cash Tool address to his address that he uses exclusively for the provision of aid. He intended to continue doing so.

52. Mr. Doe is not a terrorist or a criminal and does not intend to transact with terrorists or criminals. In the course of using the Tornado Cash Tool for his own

contributions, his assets would never come under the control of any other person or organization, including any foreign person or organization. In the course of using the Tornado Cash Tool for contributions by other American donors, their assets would never come under the control of any foreign person or organization.

53. As a result of the Biden Administration's criminalization of the Tornado Cash Tool, donations have stopped. Mr. Doe is not comfortable facilitating donations without the protection of the Tornado Cash Tool. He is not confident that any alternative tools, standing alone, will provide a sufficient level of privacy or security.

54. Plaintiff David Hoffman is a crypto asset investor and entrepreneur who resides in New York.

55. Mr. Hoffman uses Ethereum publicly. Like many users, Mr. Hoffman makes one of his Ethereum addresses public, so that anyone can access it online and transact with him.

56. After the Biden Administration criminalized the Tornado Cash Tool, an unknown person sent crypto assets to Mr. Hoffman's public address through the Tornado Cash Tool. Ethereum users like Mr. Hoffman have no ability to reject incoming transfers. So the criminalization of the Tornado Cash Tool empowered someone else to implicate Mr. Hoffman and force reporting obligations on him by causing him to receive an asset from a sanctioned entity. And it has licensed anyone else who wishes to harass or inconvenience Mr. Hoffman to continue to send crypto

assets through the Tornado Cash Tool to Mr. Hoffman's publicly known addresses, each time triggering potential liability and reporting obligations.

57. Mr. Hoffman intended to continue to use the Tornado Cash Tool in the future. He routinely uses privacy tools to protect himself while using crypto assets. Mr. Hoffman believes that the Tornado Cash Tool is a uniquely effective tool for protecting his privacy.

58. Mr. Hoffman intended to move assets from an address under his control to a Tornado Cash Tool address and then later withdraw them to a new address, also under his control. At no point would these assets have been controlled by anyone else, including any person or organization.

59. Mr. Hoffman is not a terrorist or a criminal and does not intend to transact with terrorists or criminals. And in using the Tornado Cash Tool, his assets would never come under the control of any other person or organization, including any foreign person or organization.

60. As a result of Defendants' criminalization, Mr. Hoffman is burdened with potential civil and criminal liability through no fault of his own, saddled with reporting obligations, and impeded from carrying out his intended use of the Tornado Cash Tool.

61. Defendants—Janet Yellen, in her official capacity as Secretary of the Treasury; U.S. Department of the Treasury; Andrea M. Gacki, in her official capacity as Director of the Office of Foreign Assets Control, and the Office of Foreign Assets

Control—are responsible for the enforcement and administration of the criminalization of the Tornado Cash Tool. Treasury is a federal administrative agency, and OFAC is an agency within Treasury. Both Treasury and OFAC are headquartered in Washington, D.C. Defendants acted under color of law at all relevant times.

62. The criminalization of the Tornado Cash Tool constituted final agency action.

JURISDICTION AND VENUE

63. This action arises under the Administrative Procedure Act, 5 U.S.C. §§500 et seq., and the United States Constitution.

64. This Court has jurisdiction under 28 U.S.C. §1331.

65. Venue is proper in this District under 28 U.S.C. §1391(e)(1) because Plaintiff O’Sullivan resides here and Defendants are federal agencies and officers acting in their official capacities.

BACKGROUND

66. Ethereum is a digital marketplace. It uses shared online technology to help people transact and order their finances. It hosts transactions involving cryptocurrency and other assets that use cryptographic technology.

67. Ethereum allows people to transact across long distances without middlemen. It allows people to protect against inflation by using a store of value whose supply cannot be increased by any central bank. It allows people to structure

advanced financial transactions and enforce the terms of their agreements with certainty. And it allows anyone with an internet connection to participate, regardless of their race, religion, or social status.

68. “Ethereum is arguably the most crucial platform in the crypto industry.” Yaffe-Bellany, *Crypto’s Long-Awaited ‘Merge’ Reaches the Finish Line*, N.Y. Times (Sept. 15, 2022), perma.cc/485T-2X6X. It is used by tens of millions of Americans. It facilitates transactions involving Ether, the second most common cryptocurrency in America. The present value of Ether is around \$200 billion, or about the value of McDonald’s. It also facilitates transactions involving a wide range of additional crypto assets.

69. To use Ethereum, a person creates an address, which is a personal account that only they can access and use. The address uses a pseudonym so that it can’t be immediately traced to the person who uses it.

70. Ethereum’s functionality depends on a transparent public ledger. When someone completes an Ethereum transaction, that transaction is posted to a public ledger visible to anyone, alongside his address. That transaction can’t be erased or hidden from view.

71. Although a person transacts using a pseudonymous address, there are a variety of ways to connect a person’s identity to his address. In fact, users are sometimes required by law to disclose their identity when using cryptocurrency. Once outsiders connect a person’s identity to the address that he uses, they can inspect *all* of the user’s transactions and assets.

72. Users who don't use privacy tools can therefore face risks. The transparent nature of the public ledger has allowed violent burglars to identify people holding particularly valuable crypto assets, and even torture them in front of their families until they hand over access to their crypto assets. *E.g.*, Higgins, *Man Stole \$1.8 Million in Ether After Armed Robbery, Prosecutors Say*, CoinDesk (Dec. 13, 2017), perma.cc/X8FY-NDN8; Kramer, *Dutch Bitcoin Trader Suffers Brutal Torture with a 'Heavy Drill' in Violent Robbery*, Yahoo! (Feb. 25, 2019), perma.cc/5V2C-EHBR. It can also allow unwanted snooping on private relationships and intimate transactions.

73. That's where the Tornado Cash Tool comes in. The Tornado Cash Tool allows users of cryptocurrency to protect themselves from being followed in everything that they do. It allows them to clear any discernible connection between their past transactions and their future transactions. They route an asset through a Tornado Cash Tool address and then can release it to a new, apparently unconnected address at a later date.

74. To anyone attempting to track the user, they will see that he moved some asset to a Tornado Cash Tool address, but will not know which release from that address was under his control because it will be released to a new address with no connection to the user's earlier activities. All that an outsider will see on the public ledger is something like the following:

Time 1: [1 Ether] Known User Address → Tornado Cash Tool Address

Time 2: [1 Ether] Tornado Cash Tool Address → New Address

The user himself provides, at Time 2, for the release of the asset to an address under his control or a chosen recipient's control. The user also controls how long to wait between Time 1 and Time 2. In between those two times, other users will also move and release funds from the Tornado Cash Tool, so any given user's two transactions will appear unrelated.

75. There are at least 29 addresses that make up the core of the Tornado Cash Tool. Addresses correspond to a certain fixed amount of a certain crypto asset, so each user using any given Tornado Cash Tool address will move the same amount, such as 1 unit, and then release the same amount later on. This makes each interaction with any given address look indistinguishable.

76. Throughout the duration of his use of the Tornado Cash Tool, the original user retains complete control of his assets. When he moves assets to an Tornado Cash Tool address, he retains the ability to release them at any time.

77. The Tornado Cash Tool is not like a bank that lends and invests assets once it receives them; nor does it ever mix or commingle different people's assets together. From the user's perspective, it's like a safe that keeps his asset secure and that only he can unlock.

78. No other person or organization can use or control a user's assets when that user uses this privacy tool.

79. Nobody controls the Tornado Cash Tool. It consists of computer code that executes on the user's command. Nobody can rewrite the Tornado Cash Tool

software to change how it works. And nobody can remove the Tornado Cash Tool software. It is permanent and immutable.

80. Thanks to the Tornado Cash Tool, people can use Ethereum without worrying about the safety of themselves and their families. They can keep their personal contributions and associations private. And they can rest assured that their activities will not be tracked by bad actors who might do them harm.

81. Many Ethereum users use the Tornado Cash Tool routinely to keep their assets private and secure. It is widely regarded as a good practice for anyone who wishes to participate in Ethereum responsibly.

82. Like every good technology in human history, the Tornado Cash Tool is used by some people to do bad things. The Tornado Cash Tool makes it harder to follow what all users are doing, so it makes it harder to follow what criminals are doing. But like other good technologies, it provides innumerable benefits to law-abiding Americans, and their use of the tool is understandable and appropriate.

83. For some time, it was widely believed that the United States would lead the way in embracing Ethereum and other crypto assets. Many American governors, legislators, mayors, and public figures have celebrated America's pioneering role in the use of cryptocurrency. *See, e.g., Gov. DeSantis Seeks 'Crypto Friendly' Florida*, CBS Miami (Dec. 10, 2021), perma.cc/U8TN-K2HD; Stewart, *Cryptocurrency Gets Warm Texas Welcome from Gov. Abbott*, Houston Chronicle (Jun. 22, 2021), perma.cc/LMG6-54XF;

Yaffe-Bellany, *The Rise of the Crypto Mayors*, N.Y. Times (Jan. 25, 2022), perma.cc/8ULT-GFLS.

84. But America's leading role has been thrown into reverse by the Biden Administration's recent efforts to punish crypto users. For a variety of political reasons, the Administration has sought to hyper-regulate and criminalize common uses of cryptocurrency. Klein, *How Biden's Executive Order on Cryptocurrency May Impact the Fate of Digital Currency and Assets*, Brookings (Mar. 17, 2022), perma.cc/2EZS-HYE8; Hall, *Biden Administration Targets Bitcoin Mining In New Report*, Nasdaq (Sept. 21, 2022), perma.cc/HAL6-222Z; Warmbrodt, *Elizabeth Warren's Anti-crypto Crusade Splits the Left*, Politico (Mar. 15, 2022), perma.cc/ST7F-7GBJ.

85. Perhaps no attack on the crypto world has been as severe as the August 2022 criminalization and November 2022 re-criminalization of the Tornado Cash Tool.

86. Under the International Emergency Economic Powers Act, the President can take certain actions after "declar[ing] a national emergency with respect to" an "unusual and extraordinary threat, which has its source in whole or substantial part outside the United States, to the national security, foreign policy, or economy of the United States." 50 U.S.C. §1701(a).

87. After declaring an emergency, the President can take certain actions. §1702(a)(1). As relevant here, the President can prohibit transactions subject to American jurisdiction, but only if those transactions occur "in foreign exchange" or

include “any property in which any foreign country or a national thereof has any interest.” *Id.* The President cannot prohibit transactions that include no foreign property, such as transactions among Americans or activities by a single American with respect to his own property.

88. In full, and broken down by element, the statute authorizes the President to:

investigate, block during the pendency of an investigation, regulate, direct and compel, nullify, void, prevent or prohibit

any acquisition, holding, withholding, use, transfer, withdrawal, transportation, importation or exportation of, or dealing in, or exercising any right, power, or privilege with respect to, or transactions involving,

any *property* in which *any foreign country* or a *national thereof* has any interest

by any person, or with respect to any property, subject to the jurisdiction of the United States.

§1702(a)(1)(B) (emphasis added).

89. It also authorizes the President to “investigate, regulate, or prohibit ... any transactions in foreign exchange.” *Id.* §1702(a)(1)(A).

90. Under the North Korea Sanctions and Policy Enhancement Act, the President can criminalize transactions with North Korean-related persons within the same scope. 22 U.S.C. §§9201 et seq. For instance, he can criminalize transactions involving qualifying North-Korean-related “person[s]” when those transactions are “in foreign exchange.” 22 U.S.C. §9214; *see also, e.g., id.* §9214(c), §9214(f), §9221c.

91. President Obama delegated some of his power under these statutes to the Secretary of the Treasury. Exec. Order 13694, 80 Fed. Reg. 18,077, 18,077-18,078 (Apr. 2, 2015); Exec. Order 13722, 81 Fed. Reg. 14,943, 14,495 (Mar. 18, 2016). In his Executive Orders, President Obama authorized the Secretary of the Treasury to identify “person[s]” involved in qualifying cyber-enabled activities. He then authorized the Secretary to “bloc[k]” the “property and interests in property” of any of those identified persons.

92. The Secretary of Treasury in turn delegated that authority to the Director of OFAC and enacted regulations to govern the exercise of that authority. *See* 31 C.F.R. §§578.802, 578.201 et seq.

93. As relevant here, those regulations provide that, under certain conditions, Defendants can criminalize transactions that fall within the scope of the statute. But they can do so only by designating “persons” with whom Americans cannot trade. This was the rule when the Tornado Cash Tool was criminalized, *see* 80 Fed. Reg. 81,752, 81,754 (Dec. 31, 2015), and was reaffirmed in updated regulations issued subsequent to the initial criminalization but before the withdrawal and re-criminalization, *see* 31 C.F.R. §578.201(a) (effective Sept. 6, 2022); *see also id.* §510.201.

94. The term “person” means only an “individual or entity.” *Id.* §578.313. It does not cover an idea, a tool, or a technology.

95. The Director of OFAC maintains a Specially Designated Nationals and Blocked Persons List, which in turn designates persons pursuant to these statutes.

96. Adding a person to the List criminalizes transactions with that person. If an American transacts with a person on the List, he commits a federal felony punishable by up to 20 years in prison and a \$1,000,000 fine. Americans are also required to block any property or interests in property of that designated person, and are required to report any such blocked property in their possession or control to OFAC. *See* 31 C.F.R. §578.201; *id.* §578.701; *id.* §§501.101 et seq.; *id.* §§510.201 et seq.; 87 Fed. Reg. 54,373 (Sept. 6, 2022).

97. Some earlier designations on the List include Vladimir Putin, Bashar al Assad, and the late Saddam Hussein, Qasem Soleimani, and Muammar Gaddafi. *See OFAC Specially Designated Nationals and Blocked Persons List*, perma.cc/PC4B-M7MQ.

98. As a result of these designations, it would be a felony for an American to, for example, sell a house to Vladimir Putin.

99. But on August 8, 2022, OFAC made a new and unprecedented kind of designation. It added “Tornado Cash” to the List. *See U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash*, OFAC (Aug. 8, 2022), perma.cc/8W7V-MCBP. Its designation originally included 38 Ethereum addresses.

100. In its press release, OFAC did not appear to understand what it was designating. It referred to “Tornado Cash” as a “blocked ... perso[n],” *id.*, and described its “willingness to remove” “Tornado Cash” if it demonstrated “a positive

change in behavior,” *id.*, even though it was referring to a widely available software tool, lacking agency and not controlled by anyone.

101. On October 12, 2022, Plaintiffs brought this lawsuit, alleging that the criminalization of this privacy tool exceeded Defendants’ statutory authority, was contrary to law, was arbitrary and capricious, and violated the First Amendment.

102. On November 8, 2022, Defendants withdrew their initial criminalization of the Tornado Cash Tool. They then re-criminalized it with different justification and specifications. They emphasized the Tool’s use by North-Korea-related persons. *Treasury Designates DPRK Weapons Representatives: Tornado Cash Redesignated with Additional DPRK Authorities, New OFAC Guidance*, OFAC (Nov. 8, 2022), perma.cc/V387-KEPG.

103. They continued to refer to “Tornado Cash” as a “blocked ... perso[n],” and described their “willingness to remove” “Tornado Cash” if it demonstrated “a positive change in behavior.” *Id.*

104. In a new FAQ response, Defendants acknowledged the mismatch between the requirement that they sanction “person[s]” and the designation of the Tornado Cash Tool. They attempted to overcome that mismatch by identifying persons and an organization—“founders,” “developers,” and a “decentralized autonomous organization”—who “use” the tool to advance their goals. *See Frequently Asked Questions No. 1095*, Dep’t of Treasury, perma.cc/R7RS-JBF4. But then they criminalized transactions with the Tool—not with those persons and organizations. *Id.*

105. Specifically, Defendants listed 90 Ethereum addresses, thereby criminalizing transactions involving any of those 90 addresses.

106. The 90 listed addresses include 29 addresses at issue in this lawsuit. Those 29 addresses host the technology and support functions that together constitute the core of the Tornado Cash Tool. They are identified in full in the appendix to this complaint. They allow users to move various assets and later release the same assets to a new address.

107. The other 61 listed addresses are either non-functional, serve other purposes, can be controlled by someone—such as the decentralized autonomous organization identified by Defendants—or share all of these characteristics.

108. For purposes of this lawsuit, Plaintiffs do not challenge Defendants’ claim that transactions with those 61 addresses involve qualifying foreign property and involve persons within Defendants’ authority. Plaintiffs also do not challenge Defendants’ power to criminalize transactions with any identified persons, including the founders, developers, and decentralized autonomous organization who Defendants now call “Tornado Cash.” Plaintiffs challenge only the criminalization of transactions with the 29 addresses that host the immutable Tornado Cash Tool.

109. All 90 addresses are Ethereum addresses. Defendants listed all 90 with the prefix “Digital Currency Address - ETH,” which means that they refer to addresses on only the Ethereum public ledger, and not to addresses on any other public ledger. *See* Dep’t of Treasury, *Burma-Related Designations; North Korea Designations;*

Cyber-Related Designation; Cyber-Related Designation Removal; Publication of Cyber-Related Frequently Asked Questions (Nov. 8, 2022), perma.cc/5D55-JN5Q (listing addresses); *see also* OFAC, *Sanctions List Search* (last accessed Dec. 6, 2022), perma.cc/R4LH-HWE9 (listing addresses). To the extent that Defendants meant to and later do list any identical alphanumeric addresses on other public ledgers, and those addresses also host the immutable Tornado Cash Tool, Plaintiffs challenge the criminalization of those addresses as well.

110. Each of the challenged Tornado Cash Tool addresses is immutable and operates at the user's command. They are used to complete functions that do not involve any property in which any foreign country or national thereof has any interest. The addresses are not themselves property. None is a person, none identifies a person, and none is controlled by any person. They are therefore beyond the scope of Defendants' statutory and regulatory authority to criminalize.

111. But as a result of the Biden Administration's action, using these addresses is now criminal. No Ethereum user subject to American jurisdiction can lawfully use the Tornado Cash Tool for any purpose. Plaintiffs and other law-abiding citizens are prohibited from depositing, withdrawing, sending, or receiving funds through the Tornado Cash Tool, even when the funds are lawfully obtained and being used for lawful purposes.

112. For users who had moved an asset to a Tornado Cash Tool address but not yet released it, they now cannot release their own property. *See Frequently Asked*

Questions No. 1079, Dep’t of Treasury, perma.cc/5Z68-RU5X; Fries, *OFAC Breaks Its Silence on Funds Locked with Tornado Cash*, Tokenist (Sept. 13, 2022), perma.cc/4K2K-LSLV.

113. And for all Americans, it is now a crime to use a helpful privacy tool, even though they will never transact with any foreigner or any property in which any foreigner had any interest by virtue of using that tool. *See Frequently Asked Questions No. 1077*, Dep’t of Treasury, perma.cc/77F8-VDB2.

114. For all Americans, it is now impossible to use the best tool for protecting their privacy when they engage in expressive associations with crypto assets. They are chilled from contributing to causes that they support because those contributions will now be subject to public exposure. By criminalizing this privacy tool, the Biden Administration has chilled—and in some cases altogether prevented—Americans from engaging in protected advocacy.

115. To justify its action, the Biden Administration initially explained that the Lazarus Group, a North Korean criminal organization, used the Tornado Cash Tool to cover up its theft of crypto assets.

116. It then subsequently explained that the developers and founders of the Tool, along with a decentralized autonomous organization, also “use” the Tool to advance a variety of goals.

117. But nobody—not the Lazarus Group, not the developers and founders, not the decentralized autonomous organization, and not any other foreign

organization—has control over the Tornado Cash Tool, let alone an interest in transactions that Americans make with themselves and each other using the Tornado Cash Tool.

118. Making it a crime for Americans to use the Tornado Cash Tool because the Lazarus Group or other foreign persons used the Tool to further their illicit activities is like making it a crime for Americans to use email because the Lazarus Group used email to further its illicit activities. Sometimes good tools are used by bad people. That inevitability does not justify criminalizing every American's use of those tools, and the law gives Defendants no such power.

119. The criminalization of the Tornado Cash Tool, perversely, means that foreign terrorists or developers can take down parts of the American economy by using our best technologies and ideas—a kind of cyber-age heckler's veto.

120. Worse, the criminalization of the Tornado Cash Tool does not even prevent foreign terrorists or any of the identified persons or organizations from using it. It remains online and operable, precisely because nobody can control it.

121. The criminalization of the Tornado Cash Tool has created far-reaching and embarrassing consequences. Because the Tornado Cash Tool consists of already-published, self-executing code, it is still operational. The fact that no intermediary is necessary for the Tornado Cash Tool to operate means that anyone can send unsolicited crypto assets through the Tornado Cash Tool to Americans with known Ethereum addresses. In other words, the Biden Administration has

empowered any bad actor to easily subject a law-abiding American to potential civil and criminal liability and burdensome reporting obligations, through no fault of the American's own—a phenomenon known as “dusting.”

122. And that has happened. Soon after the Biden Administration's criminalization of the Tornado Cash Tool, an unknown person or persons sent small amounts of crypto assets (“dust”) through the Tornado Cash Tool to a wide range of celebrities and publicly known users of Ethereum. Mack, *US Treasury Sanctioning Tornado Cash Unleashes 'Max Chaos' in the Crypto Universe*, Forbes (Aug. 9, 2022), perma.cc/X6PC-V7CH.

123. For example, unknown actors sent assets through the Tornado Cash Tool to Shaquille O'Neal and Jimmy Fallon. And many Americans who lack the teams of lawyers that are available to Shaquille O'Neal and Jimmy Fallon were subject to similar acts. Tan, *Someone Is Trolling Celebs by Sending ETH from Tornado Cash*, CoinDesk (Aug. 9, 2022), perma.cc/TM9H-8MJ3; Chow, *A New U.S. Crackdown Has Crypto Users Worried About Their Privacy*, Time (Aug. 10, 2022), perma.cc/6GVT-HA3R.

124. Because the law imposes strict liability, users who are “dusted” in this manner still face criminal liability and still have reporting obligations. Treasury confirmed as much in the FAQs it released on September 13, 2022 and reissued on November 8, 2022. In response to a question about dusting, the FAQs confirm that “[t]echnically, OFAC's regulations would apply to these transactions.” All that

Treasury could say is that, in its unilateral discretion, OFAC would not “prioritize enforcement” against dusted individuals whose reports were merely “delayed.”

125. Without judicial relief, the Biden Administration’s action will prevent Plaintiffs and others who are similarly situated from using the Tornado Cash Tool. Ethereum users will be forced to choose between transacting without the privacy benefits of the Tornado Cash Tool and forgoing the opportunity to engage in valuable and important uses of Ethereum. They will be chilled in their expressive activities. And they will be subject to civil and criminal liability and burdensome reporting obligations through no fault of their own.

126. The ongoing harms are immediately redressable. An order effectively requiring Defendants to decriminalize use of the Tornado Cash Tool addresses would allow Plaintiffs to conduct their legitimate activities with some measure of anonymity, use their preferred software tool without fear of penalties, and engage in important expressive associations.

127. Judicial relief would also serve the public interest by averting harm to users of the Tornado Cash Tool who are United States persons, to Ethereum as a freedom and privacy enhancing technology, and to the important sector of the economy that depends on Ethereum.

CLAIMS FOR RELIEF

Count One

Statutory Authority

5 U.S.C. §706(2)(C)

128. Plaintiffs incorporate and restate all their prior allegations.

129. Under 50 U.S.C. §1702(a), the President can prohibit “transactions in foreign exchange.” *Id.* §1702(a)(1)(A). He can also “investigate, block during the pendency of an investigation, regulate, direct and compel, nullify, void, prevent or prohibit,” “any acquisition, holding, withholding, use, transfer, withdrawal, transportation, importation or exportation of, or dealing in, or exercising any right, power, or privilege with respect to, or transactions involving,” “any property in which *any foreign country* or a *national thereof* has any interest,” “by any person, or with respect to any property, subject to the jurisdiction of the United States.” *Id.* §1702(a)(1)(B) (emphases added).

130. Under 22 U.S.C. §§9201 et seq., the President can apply this power to North Korean “persons” to restrict transactions that fall within the same scope. 22 U.S.C. §9214(c). In other words, all criminalized transactions must be in “foreign exchange” or involve “any property in which any foreign country or a national thereof,” including a North-Korea-related person, “has any interest.”

131. Americans’ use of Tornado Cash Tool addresses is not a “transaction in foreign exchange” and does not involve “any property in which any foreign country

or a national thereof has any interest.” The Tornado Cash Tool is not a North Korean “person” or any other person, organization, or entity.

132. Many uses of the Tornado Cash Tool involve only a *single* American, moving his own asset between his own addresses. Many involve transactions between two Americans. These transactions are not made in foreign exchange or with foreign property.

133. Especially given the economic and political significance of this action and its application to a technology beyond Defendants’ area of expertise, Defendants could not justify this action without a “clear congressional authorization.” *See West Virginia v. EPA*, 142 S. Ct. 2587, 2608-09 (2022); *King v. Burwell*, 576 U.S. 473, 486 (2015). Yet Congress has provided no authorization at all for this regulation of purely domestic uses of the Tornado Cash Tool.

134. The criminalization of the Tornado Cash Tool was therefore “in excess of statutory ... authority” and must be set aside. 5 U.S.C. §706(2)(C).

Count Two
Contrary to Law
5 U.S.C. §706(2)(A)

135. Plaintiffs incorporate and restate all their prior allegations

136. Under President Obama’s Executive Orders and their own regulations, Defendants can exercise power under the Act only by designating “persons,” for whom certain consequences follow. *See* Exec. Order 13694, 80 Fed. Reg. 18,077 (Apr.

2, 2015); 31 C.F.R. §578.201(a); Exec. Order 13722, 81 Fed. Reg. 14,943, 14,495 (Mar. 18, 2016); 31 C.F.R. §510.201.

137. The term “person” means only an “individual or entity.” *Id.* §§578.313, 510.322. It does not mean an idea, a tool, or a technology.

138. OFAC thinks that the privacy tool is a “blocked person[]” that can “change [its] behavior.” *See U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash*, OFAC (Aug. 8, 2022), perma.cc/FA7D-WSRG; *Treasury Designates DPRK Weapons Representatives: Tornado Cash Redesignated with Additional DPRK Authorities, New OFAC Guidance*, OFAC (Nov. 8, 2022), perma.cc/PY2P-DQDH. It is not.

139. None of the Tornado Cash Tool addresses listed by Defendants are a person. They are not individuals or entities, but rather addresses of an immutable tool beyond the control of any person or entity.

140. The criminalization of the Tornado Cash Tool was therefore “not in accordance with law” and must be set aside. 5 U.S.C. §706(2)(A).

Count Three
Arbitrary or Capricious
5 U.S.C. §706(2)(A)

141. Plaintiffs incorporate and restate all their prior allegations.

142. When an agency “entirely fail[s] to consider an important aspect of the problem,” it acts arbitrarily and capriciously. *Motor Vehicle Mfrs. Ass’n of U.S., Inc. v. State Farm*, 463 U.S. 29, 43 (1983). Defendants failed to consider three important aspects of the problem when criminalizing the Tornado Cash Tool.

143. First, Defendants failed to consider how their criminalization of the receipt of assets through the Tornado Cash Tool would subject people—including Plaintiff Hoffman and a wave of public figures—to criminal liability without any voluntary action on their own part, in violation of the Constitution and half a millennium of Anglo-Saxon common-law norms. *Robinson v. California*, 370 U.S. 660, 666 (1962).

144. Second, Defendants failed to consider how their criminalization of the Tornado Cash Tool would result in a deprivation or seizure of the assets of Americans who had moved funds to a Tornado Cash Tool address but not yet released them, without any constitutionally required process.

145. Third, Defendants failed to consider how their criminalization of a privacy tool would chill expressive associations and how their criminalization of the use of the same underlying software at different addresses would chill the right of Americans to write and publish code freely.

146. Defendants also changed their position as to whether they could sanction a technology, not controlled by any persons. When an agency changes its position, it acts arbitrarily and capriciously if it does not “display awareness that it *is* changing position” and then “show that there are good reasons for the new policy.” *F.C.C. v. Fox Television Stations, Inc.*, 556 U.S. 502, 515 (2009); *see Encino Motorcars, LLC v. Navarro*, 579 U.S. 211, 221-22 (2016).

147. Until now, it had been Defendants’ policy to not sanction technologies. 31 C.F.R. §§578.201(a), 578.313. They made this policy clear in their regulations and public statements. *See, e.g., Specially Designated Nationals and Blocked Persons List (SDN) Human Readable Lists*, OFAC, perma.cc/Q3X7-GD6X (“OFAC publishes a list of *individuals and companies* owned or controlled by, or acting for or on behalf of, targeted countries. It also lists *individuals, groups, and entities*, such as terrorists and narcotics traffickers.”) (emphases added).

148. Defendants did not “display awareness” that they were changing their position, *Fox*, 556 U.S. at 515, in sanctioning the Tornado Cash Tool. Defendants in fact appear to continue to believe that the Tornado Cash Tool is a “perso[n],” *see U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash*, OFAC (Aug. 8, 2022), perma.cc/S5R3-XW4X, or is identical to the “person[s]” who “use” it but have no control over it, *Treasury Designates DPRK Weapons Representatives: Tornado Cash Redesignated with Additional DPRK Authorities, New OFAC Guidance*, OFAC (Nov. 8, 2022), perma.cc/R56Z-P5YR

149. Nor did Defendants “show that there are good reasons for the new policy.” They provided no reasons at all for the change in course.

150. Next, Defendants acted pretextually in sanctioning the Tornado Cash Tool. When there is a “significant mismatch between the decision [an agency] made and the rationale [it] provided,” the agency acts arbitrarily and capriciously. *Dep’t of Com. v. New York*, 139 S. Ct. 2551, 2575 (2019). Defendants were “determined” to

sanction the Tornado Cash Tool to advance their domestic policy agenda. *Id.* at 2574. Although their rationale for sanctioning the Tornado Cash Tool was that certain developers, founders, and a decentralized autonomous organization qualified as “person[s]” subject to sanction, they did not sanction transactions with any of those persons or that organization. Instead, they sanctioned only transactions with the Tool itself, even though those persons and that organization have no control over Americans’ use of the Tool. Likewise, although foreign terrorist groups have used the Tool, they can continue to do so after the designation. Defendants’ shifting rationales for the same outcome—making it illegal for Americans to protect their privacy—underscores the pretext here.

151. Finally, Defendants simply disregarded their own rules requiring that they exercise their sanction power only by designating “persons.” 31 C.F.R. §578.201(a) (“persons”); *id.* §578.313 (“individual or entity”); *id.* §§510.201 et seq. (same). When an agency “simply disregard[s] rules that are still on the books,” it acts arbitrarily and capriciously. *Fox*, 556 U.S. at 515.

152. For all these reasons and more, the criminalization of the Tornado Cash Tool was “arbitrary” or “capricious” and must be set aside. 5 U.S.C. §706(2)(A).

Count Four

First Amendment

5 U.S.C. §706(2)(A), (B); U.S. Const., amend. I

153. Plaintiffs incorporate and restate all their prior allegations.

154. The First Amendment protects Americans’ freedom to associate for “a wide variety of political, social, economic, educational, religious, and cultural ends.” *Roberts v. U.S. Jaycees*, 468 U.S. 609, 622 (1984). And freedom of association includes a right to associational privacy. There is a “vital relationship between freedom to associate and privacy in one’s associations.” *Ams. for Prosperity Found. v. Bonta*, 141 S. Ct. 2373, 2382 (2021).

155. Infringements on associational privacy “chill[] speech by exposing anonymous donors to harassment and threats of reprisal.” *Del. Strong Fams. v. Denn*, 136 S. Ct. 2376, 2376 (2016) (Thomas, J., dissent). Individuals have a “strong associational interest in maintaining the privacy of” their associational activities. *Gibson v. Fla. Legis. Investigation Comm.*, 372 U.S. 539, 555-56 (1963). “Inviolability of privacy in group association” is “indispensable to preservation of freedom of association.” *Bates v. City of Little Rock*, 361 U.S. 516, 523 (1960).

156. The criminalization of the Tornado Cash Tool infringes on associational privacy by outlawing the use of an essential privacy tool and forcing users of that tool to disclose their activities to the federal government and the public. It thereby chills the associational activities of Mr. Doe, Coin Center, and their donors.

157. Defendants’ criminalization of the Tornado Cash Tool was therefore “not in accordance with law” and “contrary to constitutional right” and must be set aside. 5 U.S.C. §706(2)(A), (B).

PRAYER FOR RELIEF

Plaintiffs respectfully request that the Court grant the following relief:

- A. A declaration that the criminalization of the Tornado Cash Tool is null, void, and with no force or effect;
- B. A declaration that the criminalization of the Tornado Cash Tool is not in accordance with law under 5 U.S.C. §706(2)(A); is contrary to constitutional right under §706(2)(B); is arbitrary and capricious under §706(2)(A); and is in excess of statutory jurisdiction, authority, or limitations under §706(2)(C);
- C. An order vacating and setting aside the criminalization of the Tornado Cash Tool.
- D. An injunction preventing Defendants and their officers, employees, or agents from enforcing, implementing, applying, or taking any action whatsoever under, or in reliance on, the criminalization of the Tornado Cash Tool.
- E. An order awarding Plaintiffs their costs in this action, including attorneys' fees;
- F. Any other relief that the Court deems just and proper, including relief as to any other public ledger addresses that host the Tornado Cash Tool that Defendants criminalize.

Respectfully submitted,

s/ Cameron T. Norris

Michael A. Sasso
Florida Bar No. 93814
masasso@sasso-law.com
Christian Bonta
Florida Bar No. 1010347
cbonta@sasso-law.com
SASSO & SASSO, P.A.
1031 West Morse Blvd, Suite 120
Winter Park, Florida 32789
Tel.: (407) 644-7161

Jeffrey M. Harris*
Cameron T. Norris*
Jeffrey S. Hetzel*
CONSOVOY MCCARTHY PLLC
1600 Wilson Boulevard, Suite 700
Arlington, VA 22209
Telephone: 703.243.9423

J. Abraham Sutherland*
106 Connally Street
Black Mountain, NC 28711
Telephone: 805.689.4577

Dated: December 8, 2022

Attorneys for Plaintiffs

* *Pro hac vice*.

Appendix: Sanctioned Addresses

Immutable and Challenged in this Lawsuit

	Sanctioned Address
1	Digital Currency Address - ETH 0x12D66f87A04A9E220743712cE6d9bB1B5616B8Fc
2	Digital Currency Address - ETH 0x47CE0C6eD5B0Ce3d3A51fdb1C52DC66a7c3c2936
3	Digital Currency Address - ETH 0x910Cbd523D972eb0a6f4cAe4618aD62622b39DbF
4	Digital Currency Address - ETH 0xA160cdAB225685dA1d56aa342Ad8841c3b53f291
5	Digital Currency Address - ETH 0xD4B88Df4D29F5CedD6857912842cff3b20C8Cfa3
6	Digital Currency Address - ETH 0xFD8610d20aA15b7B2E3Be39B396a1bC3516c7144
7	Digital Currency Address - ETH 0x07687e702b410Fa43f4cB4Af7FA097918ffD2730
8	Digital Currency Address - ETH 0x23773E65ed146A459791799d01336DB287f25334
9	Digital Currency Address - ETH 0x22aaA7720ddd5388A3c0A3333430953C68f1849b
10	Digital Currency Address - ETH 0xBA214C1c1928a32Bffe790263E38B4Af9bFCD659
11	Digital Currency Address - ETH 0x03893a7c7463AE47D46bc7f091665f1893656003
12	Digital Currency Address - ETH 0x2717c5e28cf931547B621a5dddb772Ab6A35B701
13	Digital Currency Address - ETH 0xD21be7248e0197Ee08E0c20D4a96DEBdaC3D20Af
14	Digital Currency Address - ETH 0x4736dCf1b7A3d580672CcE6E7c65cd5cc9cFBa9D
15	Digital Currency Address - ETH 0xd96f2B1c14Db8458374d9Aca76E26c3D18364307
16	Digital Currency Address - ETH 0x169AD27A470D064DEDE56a2D3ff727986b15D52B
17	Digital Currency Address - ETH 0x0836222F2B2B24A3F36f98668Ed8F0B38D1a872f
18	Digital Currency Address - ETH 0x178169B423a011fff22B9e3F3abeA13414dDD0F1
19	Digital Currency Address - ETH 0x610B717796ad172B316836AC95a2ffad065CeaB4
20	Digital Currency Address - ETH 0xbB93e510BbCD0B7beb5A853875f9eC60275CF498
21	Digital Currency Address - ETH 0xCEe71753C9820f063b38FDbE4cFDAf1d3D928A80
22	Digital Currency Address - ETH 0x756C4628E57F7e7f8a459EC2752968360Cf4D1AA

23	Digital Currency Address - ETH 0x94C92F096437ab9958fC0A37F09348f30389Ae79
24	Digital Currency Address - ETH 0xD82ed8786D7c69DC7e052F7A542AB047971E73d2
25	Digital Currency Address - ETH 0x88fd245fEdeC4A936e700f9173454D1931B4C307
26	Digital Currency Address - ETH 0x653477c392c16b0765603074f157314Cc4f40c32
27	Digital Currency Address - ETH 0x743494b60097A2230018079c02fe21a7B687EAA5
28	Digital Currency Address - ETH 0xDF3A408c53E5078af6e8fb2A85088D46Ee09A61b
29	Digital Currency Address - ETH 0x09193888b3f38C82dEdfda55259A82C0E7De875E

Not Challenged in this Lawsuit

	Sanctioned Address
30	Digital Currency Address - ETH 0xd90e2f925DA726b50C4Ed8D0Fb90Ad053324F31b
31	Digital Currency Address - ETH 0x58E8dCC13BE9780fC42E8723D8EaD4CF46943dF2
32	Digital Currency Address - ETH 0x527653eA119F3E6a1F5BD18fbF4714081D7B31ce
33	Digital Currency Address - ETH 0xCa0840578f57fE71599D29375e16783424023357
34	Digital Currency Address - ETH 0x722122dF12D4e14e13Ac3b6895a86e84145b6967
35	Digital Currency Address - ETH 0x905b63Fff465B9fFBF41DeA908CEb12478ec7601
36	Digital Currency Address - ETH 0x94A1B5CdB22c43faab4AbEb5c74999895464Ddaf
37	Digital Currency Address - ETH 0xb541fc07bC7619fD4062A54d96268525cBC6FfEF
38	Digital Currency Address - ETH 0xF60dD140cFf0706bAE9Cd734Ac3ae76AD9eBC32A
39	Digital Currency Address - ETH 0xb1C8094B234DcE6e03f10a5b673c1d8C69739A00
40	Digital Currency Address - ETH 0xD691F27f38B395864Ea86CfC7253969B409c362d
41	Digital Currency Address - ETH 0xaEaaC358560e11f52454D997AAFF2c5731B6f8a6
42	Digital Currency Address - ETH 0x1356c899D8C9467C7f71C195612F8A395aBf2f0a
43	Digital Currency Address - ETH 0xA60C772958a3eD56c1F15dD055bA37AC8e523a0D
44	Digital Currency Address - ETH 0xF67721A2D8F736E75a49FdD7FAd2e31D8676542a
45	Digital Currency Address - ETH 0x9AD122c22B14202B4490eDAf288FDdb3C7cb3ff5E

46	Digital Currency Address - ETH 0xDD4c48C0B24039969fC16D1cdF626eaB821d3384
47	Digital Currency Address - ETH 0x8589427373D6D84E98730D7795D8f6f8731FDA16
48	Digital Currency Address - ETH 0x84443CFd09A48AF6eF360C6976C5392aC5023a1F
49	Digital Currency Address - ETH 0x330bdFADE01eE9bF63C209Ee33102DD334618e0a
50	Digital Currency Address - ETH 0xaf4c0B70B2Ea9FB7487C7CbB37aDa259579fe040
51	Digital Currency Address - ETH 0x1E34A77868E19A6647b1f2F47B51ed72dEDE95DD
52	Digital Currency Address - ETH 0xa5C2254e4253490C54cef0a4347fddb8f75A4998
53	Digital Currency Address - ETH 0xdf231d99Ff8b6c6CBF4E9B9a945CBAcEF9339178
54	Digital Currency Address - ETH 0xaf8d1839c3c67cf571aa74B5c12398d4901147B3
55	Digital Currency Address - ETH 0xffbac21a641dcfe4552920138d90f3638b3c9fba
56	Digital Currency Address - ETH 0x3efa30704d2b8bbac821307230376556cf8cc39e
57	Digital Currency Address - ETH 0x179f48c78f57a3a78f0608cc9197b8972921d1d2
58	Digital Currency Address - ETH 0xd47438c816c9e7f2e2888e060936a499af9582b3
59	Digital Currency Address - ETH 0xb04E030140b30C27bcdfaaFFFA98C57d80eDa7B4
60	Digital Currency Address - ETH 0x5f6c97C6AD7bdd0AE7E0Dd4ca33A4ED3fDabD4D7
61	Digital Currency Address - ETH 0xf4B067dD14e95Bab89Be928c07Cb22E3c94E0DAA
62	Digital Currency Address - ETH 0xB20c66C4DE72433F3cE747b58B86830c459CA911
63	Digital Currency Address - ETH 0x2FC93484614a34f26F7970CBB94615bA109BB4bf
64	Digital Currency Address - ETH 0x5efda50f22d34F262c29268506C5Fa42cB56A1Ce
65	Digital Currency Address - ETH 0xD692Fd2D0b2Fbd2e52CFa5B5b9424bC981C30696
66	Digital Currency Address - ETH 0x2f50508a8a3d323b91336fa3ea6ae50e55f32185
67	Digital Currency Address - ETH 0x2573BAc39EBE2901B4389CD468F2872cF7767FAF
68	Digital Currency Address - ETH 0x746aebc06d2ae31b71ac51429a19d54e797878e9
69	Digital Currency Address - ETH 0x01e2919679362dFBC9ee1644Ba9C6da6D6245BB1
70	Digital Currency Address - ETH 0x5cab7692D4E94096462119ab7bF57319726Eed2A
71	Digital Currency Address - ETH 0x77777feddddffc19ff86db637967013e6c6a116c

72	Digital Currency Address - ETH 0x26903a5a198D571422b2b4EA08b56a37cbD68c89
73	Digital Currency Address - ETH 0x6Bf694a291DF3FeC1f7e69701E3ab6c592435Ae7
74	Digital Currency Address - ETH 0x242654336ca2205714071898f67E254EB49ACdCe
75	Digital Currency Address - ETH 0x3aac1cC67c2ec5Db4eA850957b967Ba153aD6279
76	Digital Currency Address - ETH 0x776198CCF446DFa168347089d7338879273172cF
77	Digital Currency Address - ETH 0xCC84179FFD19A1627E79F8648d09e095252Bc418
78	Digital Currency Address - ETH 0x723B78e67497E85279CB204544566F4dC5d2acA0
79	Digital Currency Address - ETH 0xeDC5d01286f99A066559F60a585406f3878a033e
80	Digital Currency Address - ETH 0xD5d6f8D9e784d0e26222ad3834500801a68D027D
81	Digital Currency Address - ETH 0x76D85B4C0Fc497EeCc38902397aC608000A06607
82	Digital Currency Address - ETH 0x0E3A09dDA6B20aFbB34aC7cD4A6881493f3E7bf7
83	Digital Currency Address - ETH 0x05E0b5B40B7b66098C2161A5EE11C5740A3A7C45
84	Digital Currency Address - ETH 0x538Ab61E8A9fc1b2f93b3dd9011d662d89bE6FE6
85	Digital Currency Address - ETH 0x407CcEeaA7c95d2FE2250Bf9F2c105aA7AAFB512
86	Digital Currency Address - ETH 0x23173fE8b96A4Ad8d2E17fB83EA5dccccdCa1Ae52
87	Digital Currency Address - ETH 0x94Be88213a387E992Dd87DE56950a9aef34b9448
88	Digital Currency Address - ETH 0x57b2B8c82F065de8Ef5573f9730fC1449B403C9f
89	Digital Currency Address - ETH 0x8281Aa6795aDE17C8973e1aedcA380258Bc124F9
90	Digital Currency Address - ETH 0x833481186f16Cece3f1Eeea1a694c42034c3a0dB
91	Digital Currency Address - ETH 0xd8D7DE3349ccaA0Fde6298fe6D7b7d0d34586193

TAB 17

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF FLORIDA
PENSACOLA DIVISION**

COIN CENTER *et al.*,
Plaintiffs,

v.

YELLEN *et al.*,
Defendants.

Case No.
3:22-cv-20375-TKW-ZCB

ANSWER

Defendants Department of the Treasury; Office of Foreign Assets Control; Janet Yellen, in her official capacity as Secretary of the Treasury; and Andrea M. Gacki, in her official capacity as Director of the Office of Foreign Assets Control, hereby answer Plaintiffs' Amended Complaint (the "Amended Complaint"), ECF No. 21.

The introductory paragraph consists of Plaintiffs' characterization of this action, to which no response is required.

1. The allegations in this paragraph consist of Plaintiffs' characterization of this action and Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants deny the allegations in this paragraph and admit only that OFAC added Tornado Cash to the Specially Designated Nationals and Blocked

Persons (“SDN”) List on August 8, 2022, and that OFAC redesignated Tornado Cash and updated the SDN List entry on November 8, 2022, and at the same time withdrew the August 8, 2022 designation. Defendants respectfully refer the court to the designations themselves for a complete and accurate reflection of their contents. See Cyber-related Designation (Aug. 8, 2022) <https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20220808>; Burma-related Designations; North Korea Designations; Cyber-related Designation; Cyber-related Designation Removal; Publication of Cyber-related Frequently Asked Questions (Nov. 8, 2022); see also 87 Fed. Reg. 49,652 (Aug. 11, 2022); 87 Fed. Reg. 68,578 (Nov. 15, 2022). Defendants deny that the challenged designation constituted “criminaliz[ation]” and deny that characterization of Defendants’ action as it is used throughout the Amended Complaint.

2. Defendants lack knowledge or information sufficient to form a belief as to the truth of the allegations in the first sentence of this paragraph. As to the second sentence, Defendants admit only that users of the Ethereum blockchain can send and receive certain digital assets without the involvement of a traditional financial institution. Defendants otherwise deny the second sentence. Defendants admit the third sentence, and lack knowledge or information sufficient to admit or deny the fourth sentence.

3. Defendants admit the first and second sentences of this paragraph. As to the third sentence, Defendants admit only that transactions on the Ethereum blockchain cannot be erased from the public ledger, but otherwise lack knowledge and information sufficient to admit or deny the third sentence, because the phrase “hidden from view” is vague and undefined. As to the fourth sentence, Defendants admit only that users may transact on the Ethereum blockchain using digital currency addresses that need not be associated with particular individual’s identifying information, and that, in some circumstances, transactions conducted on the Ethereum blockchain platform may be linked to the individual or entity that executed such transactions. Defendants otherwise lack knowledge or information sufficient to admit or deny the fourth sentence, because the phrases “connect a person’s identity to his address on the public ledger” and “all his transactions and assets” are vague and undefined.
4. As to the allegations in this paragraph, Defendants admit only that, in some circumstances, transactions conducted on the Ethereum blockchain platform may be linked to the individual or entity that executed such transactions. Defendants otherwise lack knowledge or information sufficient to admit or deny, because the phrases “proactive steps,” “allows strangers to track his private associations and stalk his intimate relations,” “invites,” “unpopular

causes,” “a lot of assets,” and “target on his back” are vague and undefined.

5. As to the first sentence of this paragraph, Defendants lack knowledge or information sufficient to admit or deny, because the phrases “protect themselves” and “employ privacy tools” are vague and undefined.
6. The first sentence of this paragraph reflects Plaintiffs’ opinion as to what is “state-of-the-art,” which is vague and undefined, and uses the term “Tornado Cash Tool,” which is also vague and undefined, so Defendants lack knowledge or information sufficient to admit or deny those aspects of the sentence. To the extent that Plaintiffs’ use of the phrase “Tornado Cash Tool” throughout the Amended Complaint is intended to reflect Plaintiffs’ legal conclusion that certain aspects of Defendants’ designation were unlawful, that phrase constitutes a legal conclusion to which no response is required, but to the extent one is deemed required, Defendants deny the allegation. Defendants incorporate this denial, to the extent necessary, throughout this Answer, as applied to each use of the term “Tornado Cash Tool” throughout the Amended Complaint, and hereafter treat each reference to “Tornado Cash Tool” as a reference to “Tornado Cash” throughout, unless otherwise specified. As to the remainder of the first sentence, Defendants admit only that Tornado Cash facilitates anonymous transactions by obfuscating their origin, destination, and counterparties, and otherwise deny.

As to the second sentence, Defendants admit only that Tornado Cash relies upon its smart contract software, which is stored on the Ethereum blockchain at Ethereum addresses, and otherwise deny. The third and fourth sentences are admitted. Defendants deny the fifth sentence.

7. As to the first sentence of this paragraph, Defendants admit only that Tornado Cash facilitates anonymous transactions by obfuscating their origin, destination, and counterparties, and otherwise deny. The second and third sentences are denied.
8. The first and second sentences of this paragraph are denied. As for the third sentence, Defendants admit only that Tornado Cash relies upon its software, in the form of smart contracts available at particular Ethereum addresses, but otherwise deny. The fourth and fifth sentences are denied.
9. As to the first sentence of this paragraph, Defendants admit only that certain cryptocurrencies, including Bitcoin, rely on public confirmation of their transactions, which cannot be canceled, withdrawn, altered, or rescinded, but otherwise lack knowledge or information sufficient to admit or deny what cryptocurrencies are “like Bitcoin,” what those cryptocurrencies “are known, in part, for,” or whether transactions with such currencies are “irreversible,” as these phrases are vague and undefined. As for the second sentence, Defendants admit that certain cryptocurrency transactions are colloquially

referred to as “immutable,” but deny that this characterization is universally accurate, and otherwise deny. As to the third sentence, Defendants admit only that Ethereum allows individuals to publish software to its ledger, and that such software can be published in a form that disallows further editing, but otherwise deny. As to the fourth sentence, Defendants admit only that that when certain software on the Ethereum blockchain receives instructions to run, such code generally runs, and otherwise deny. The fifth sentence is denied.

10. With respect to the first sentence, Defendants admit only that Tornado Cash’s smart contracts provide the same functionality to all users, but otherwise deny the sentence. As to the second sentence, Defendants admit only that certain Tornado Cash smart contracts are designed to disallow future edits to their code, but otherwise deny. As to the third sentence, Defendants admit only that the Tornado Cash Decentralized Autonomous Organization (“DAO”) is responsible for voting on and implementing new features created by Tornado Cash developers, but otherwise deny.
11. The allegations in this paragraph consist of Plaintiffs’ characterization of the International Emergency Economic Powers Act of 1977 (“IEEPA”). Defendants respectfully refer the Court to the statute and deny any allegations that are inconsistent with it. Defendants lack knowledge or

information sufficient to admit or deny whether IEEPA is the “statutory descendant” of the Trading with the Enemy Act of 1917, because that phrase is vague and undefined.

12. The allegations in this paragraph consist of Plaintiffs’ characterization of IEEPA, which is a legal conclusion to which no response is required. To the extent a response is deemed required, Defendants admit that the cited statute contains the quoted language, but otherwise respectfully refer the Court to the statute and deny any allegations that are inconsistent with it.
13. The allegations in this paragraph consist of Plaintiffs’ characterization of IEEPA, which is a legal conclusion to which no response is required. To the extent a response is deemed required, Defendants admit that the cited statute contains the quoted language, but otherwise respectfully refer the Court to the statute and deny any allegations that are inconsistent with it.
14. The allegations in this paragraph consist of Plaintiffs’ characterization of the North Korea Sanctions and Policy Enhancement Act, which is a legal conclusion to which no response is required. To the extent a response is deemed required, Defendants admit that the cited statute contains the quoted language, but otherwise respectfully refer the Court to the statute and deny any allegations that are inconsistent with it.
15. This paragraph contains Plaintiffs’ characterization of OFAC regulations,

which is a legal conclusion to which no response is required. To the extent a response is deemed required, Defendants admit that the quoted language appears in the regulations, but otherwise respectfully refer the Court to the regulations and deny that Plaintiffs' characterization is a complete and accurate statement of their contents.

16. The allegations in the first sentence of this paragraph are denied. The second sentence is Plaintiffs' characterization of this action (because it relies upon Plaintiffs' own definition of "Tornado Cash Tool," which appears to refer to the list of addresses in the Appendix to the Amended Complaint), to which no response is required. To the extent a response is deemed required, Defendants admit only that 20 of the 38 addresses listed in the August 8 designation appear in the Appendix to the Amended Complaint, as "Challenged in this Lawsuit," but otherwise deny.
17. As to the first sentence of this paragraph, Defendants admit only that OFAC withdrew the August 8, 2022 designation and simultaneously redesignated Tornado Cash on November 8, 2022, which occurred after this lawsuit was originally filed, but otherwise deny the allegations. With respect to the second and third sentences, Defendants admit only that the November 8 designation included a list of 90 Ethereum addresses, 29 of which are listed as "Challenged in this Lawsuit" in the Appendix to the Amended Complaint,

but otherwise deny.

18. The allegations in this paragraph consist of Plaintiffs' characterization of this action, to which no response is required. To the extent a response is deemed required, Defendants admit only that 29 addresses are listed as "Challenged in this Lawsuit" in the Appendix to the Amended Complaint, but otherwise deny the allegations.
19. This paragraph consists of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants respond as follows: With respect to the first sentence of this paragraph, Defendants admit only that on November 8, 2022, OFAC delisted and simultaneously redesignated Tornado Cash under Executive Orders 13722 and 13694, as amended, and that the redesignation took into account additional information and included an additional basis for the designation of Tornado Cash regarding its support for Democratic People's Republic of Korea (DPRK) activities. Defendants otherwise deny the allegations in this paragraph, to the extent a response is deemed required.
20. The first sentence of this paragraph consists of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants deny the allegations. The remainder of this paragraph contains Plaintiffs' characterization of FAQ No. 1095, to which no

response is required. To the extent a response is deemed required, Defendants admit only that the quoted language is found in the FAQ, but otherwise deny the remaining allegations, and respectfully refer the Court to the FAQ for a complete and accurate statement of its contents.

21. This paragraph contains Plaintiffs' characterization of FAQ No. 1095 and the designation of Tornado Cash, to which no response is required. To the extent a response is deemed required, Defendants deny the allegations, and respectfully refer the Court to the FAQ and designation for a complete and accurate statement of its contents.
22. This paragraph consists of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants deny the allegations.
23. This paragraph consists of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants deny the allegations.
24. This paragraph consists of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants deny the allegations.
25. This paragraph consists of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response is deemed

required, Defendants admit only that the cited statutes contain the quoted language, but otherwise respectfully refer the Court to the statutes for a complete and accurate statement of their contents, and deny the remaining allegations.

26. This paragraph consists of Plaintiffs' legal argument and legal conclusions, and their characterization of Defendants' designation and this suit, to which no response is required. To the extent a response is deemed required, Defendants admit only that the cited regulations contain the quoted language, but otherwise respectfully refer the Court to the regulations and the designation for a complete and accurate statement of their contents, and deny the remaining allegations.
27. This paragraph consists of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants deny the allegations.
28. This paragraph consists of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants deny the allegations.
29. Defendants lack knowledge or information sufficient to admit or deny the first clause of this paragraph. The second clause consists of Plaintiffs' legal argument and legal conclusions, to which no response is required, but to the

extent a response is deemed required, Defendants respectfully refer the Court to the designation itself for a complete and accurate reflection of its contents, and deny the allegations to the extent they are inconsistent with the designation.

30. This paragraph consists of Plaintiffs' characterization of this action, as well as their legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants deny the allegations and deny that Plaintiffs are entitled to any relief.
31. Defendants lack knowledge or information sufficient to form a belief as to the truth of these allegations.
32. Defendants lack knowledge or information sufficient to form a belief as to the truth of these allegations.
33. Defendants lack knowledge or information sufficient to form a belief as to the truth of these allegations.
34. Defendants lack knowledge or information sufficient to form a belief as to the truth of these allegations.
35. Defendants lack knowledge or information sufficient to form a belief as to the truth of the allegation in the first sentence of this paragraph, but deny Plaintiffs' characterization of Defendants' action as "the Biden Administration's criminalization of the Tornado Cash Tool." The second

sentence consists of Plaintiffs' legal argument and legal conclusions, to which no response is required, but to the extent a response is required, Defendants deny the allegations. The third sentence consists of Plaintiffs' characterization of this action and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants deny the allegations in the third sentence. The fourth sentence constitutes Plaintiffs' opinion, to which no response is required. To the extent a response is deemed required, Defendants lack knowledge or information sufficient to admit or deny the allegations in this sentence.

36. Defendants lack knowledge or information sufficient to form a belief as to the truth of the allegation in the first sentence of this paragraph. The second sentence is vague, because it does not define the phrase "come under the control," but it appears to consist of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent one is required, Defendants deny the allegations in the second sentence.
37. Defendants lack knowledge or information sufficient to form a belief as to the truth of these allegations.
38. Defendants lack knowledge or information sufficient to form a belief as to the truth of these allegations.
39. Defendants lack knowledge or information sufficient to form a belief as to

the truth of these allegations.

40. Defendants lack knowledge or information sufficient to form a belief as to the truth of these allegations.
41. Defendants lack knowledge or information sufficient to form a belief as to the truth of these allegations.
42. Defendants lack knowledge or information sufficient to form a belief as to the truth of the allegations in the first sentence of this paragraph. The second sentence is vague, because it does not define the term “control,” but it appears to consist of Plaintiffs’ legal argument and legal conclusions, to which no response is required. To the extent one is required, Defendants deny the allegations in the second sentence.
43. Defendants lack knowledge or information sufficient to form a belief as to the truth of the allegations in the first and second sentences of this paragraph. The third sentence is vague, because it does not define the phrase “under the control,” but it appears to consist of Plaintiffs’ legal argument and legal conclusions, to which no response is required. To the extent one is required, Defendants deny the allegations in the third sentence.
44. Defendants lack knowledge or information sufficient to form a belief as to the truth of these allegations.
45. Defendants lack knowledge or information sufficient to form a belief as to

the truth of these allegations.

46. Defendants lack knowledge or information sufficient to form a belief as to the truth of these allegations.

47. Defendants lack knowledge or information sufficient to form a belief as to the truth of these allegations.

48. The first sentence of this paragraph constitutes Plaintiffs' opinion, to which no response is required. To the extent a response is deemed required, Defendants lack knowledge or information sufficient to admit or deny the allegations in the sentence, because it contains vague and undefined terms such as "[c]rypto donations to Ukraine" and "substantial positive impact." As to the remainder of this paragraph, Defendants admit that the cited hearing testimony contains the quoted language, but otherwise respectfully refer the Court to the hearing testimony for a complete and accurate statement of its contents. *See* "Toomey: Ukraine is Actively Utilizing Crypto to Save Lives" (Mar. 17, 2022), <https://www.banking.senate.gov/newsroom/minority/toomey-ukraine-is-actively-utilizing-crypto-to-save-lives>

49. Defendants lack knowledge or information sufficient to form a belief as to the truth of these allegations.

50. Defendants lack knowledge or information sufficient to form a belief as to

the truth of these allegations.

51. Defendants lack knowledge or information sufficient to form a belief as to the truth of these allegations.
52. Defendants lack knowledge or information sufficient to form a belief as to the truth of the allegations in the first sentence of this paragraph. The second and third sentences are vague, because they do not define the phrase “under the control,” but they appear to consist of Plaintiffs’ legal argument and legal conclusions, to which no response is required. To the extent one is required, Defendants deny the allegations in those sentences.
53. Defendants lack knowledge or information sufficient to form a belief as to the truth of these allegations, but deny Plaintiffs’ characterization of the challenged action as “the Biden Administration’s criminalization of the Tornado Cash Tool.”
54. Defendants lack knowledge or information sufficient to form a belief as to the truth of these allegations.
55. Defendants lack knowledge or information sufficient to form a belief as to the truth of these allegations.
56. Defendants lack knowledge or information sufficient to form a belief as to the truth of the allegations in the first sentence of this paragraph, but deny Plaintiffs’ characterization of the challenged action as “the Biden

Administration’s criminalization of the Tornado Cash Tool.” As to the second sentence, Defendants admit that Ethereum users generally have no ability to reject incoming transfers of cryptocurrency, but Defendants lack knowledge or information sufficient to admit or deny the remaining allegations in the second sentence. As to the third sentence, it consists of legal argument and legal conclusions to which no response is required. To the extent a response is deemed required, Defendants admit only that Tornado Cash is a sanctioned entity, and that, in general, when a U.S. person receives assets from a person named on the SDN List, such assets must be blocked and reported to OFAC, and otherwise deny. The fourth sentence constitutes Plaintiffs’ opinion, as well as legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants admit only that, in general, when a U.S. person receives assets from a person named on the SDN List, such assets must be blocked and reported to OFAC, and otherwise deny the allegations.

57. Defendants lack knowledge or information sufficient to form a belief as to the truth of these allegations.
58. Defendants lack knowledge or information sufficient to form a belief as to the truth of the allegations in the first sentence. The second sentence is vague, because it does not define the term “control,” but it appears to consist

of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent one is required, Defendants deny the allegations in the second sentence.

59. Defendants lack knowledge or information sufficient to form a belief as to the truth of the allegations in the first sentence of this paragraph. The second sentence is vague, because it does not define the phrase "come under the control," but it appears to consist of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent one is required, Defendants deny the allegations in the second sentence.
60. This paragraph consists of Plaintiffs' characterization of this action and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants admit only that Tornado Cash is a sanctioned entity, and that, in general, when a U.S. person receives assets from a person named on the SDN List, such assets must be blocked and reported to OFAC, and otherwise deny the allegations.
61. The first sentence of this paragraph consists of legal conclusions to which no response is required. To the extent a response is deemed required, admit that the listed Defendants hold the stated positions, but otherwise deny the allegations. The second, third, and fourth sentences consist of legal conclusions to which no response is required. To the extent a response is

deemed required, admitted.

62. This paragraph consists of a legal conclusion and Plaintiffs' characterization of this action, to which no response is required. To the extent a response is deemed required, deny.
63. This paragraph consists of Plaintiffs' characterization of this action and legal conclusions regarding jurisdiction, to which no response is required. To the extent a response is deemed required, Defendants admit that Plaintiffs' Amended Complaint invokes the Constitution and the Administrative Procedure Act ("APA").
64. This paragraph consists of Plaintiffs' characterization of this action and legal conclusions regarding jurisdiction, to which no response is required. To the extent a response is deemed required, Defendants admit that Plaintiffs' Amended Complaint invokes 28 U.S.C. § 1331, but deny that this Court has jurisdiction.
65. This paragraph consists of Plaintiffs' legal conclusions regarding venue, to which no response is required. To the extent a response is deemed required, Defendants are without sufficient knowledge or information to admit or deny the allegation because they lack sufficient information regarding Plaintiff O'Sullivan's residence.
66. As to the allegations in this paragraph, Defendants admit only that Ethereum

is a blockchain platform that includes a public ledger of linked data blocks and cryptographic elements, that users of the Ethereum blockchain platform can transfer digital assets between digital currency addresses, and that such addresses need not be associated with particular individuals' identifying information. Defendants otherwise lack knowledge or information sufficient to admit or deny, because the paragraph contains phrases that are vague and undefined, such as "digital marketplace," "order their finances," and "hosts transactions."

67. As to the first sentence of this paragraph, Defendants admit only that Ethereum users may transact using the Ethereum blockchain platform across long distances, but otherwise deny the allegations. The second and third sentences constitute Plaintiffs' opinion, to which no response is required. To the extent a response is deemed required, Defendants lack knowledge or information sufficient to admit or deny the allegations in the second and third sentences, because they contain vague and undefined phrases such as "protect against inflation," "store of value," "structure advanced financial transactions," and "enforce the terms of their agreements with certainty." Defendants deny the allegations in the fourth sentence.
68. With respect to the first sentence of this paragraph, Defendants admit only that the quoted language appears in the cited article, and respectfully refer the

Court to the article for a complete and accurate statement of its contents.

Defendants lack sufficient information to admit or deny the second sentence.

As to the third sentence, Defendants admit only that the Ethereum blockchain platform, among other things, facilitates transactions involving Ether, and lack knowledge or information sufficient to admit or deny the remainder of the sentence, because the term “most common” is vague and undefined.

Defendants deny the fourth sentence. Defendants lack sufficient information to admit or deny the fifth sentence because the phrase “wide range” is vague and undefined, but admit only that Ethereum supports transactions in crypto assets other than Ether.

69. As to the first sentence in this paragraph, Defendants admit only that users of Ethereum obtain addresses that correspond to accounts, but deny that all such accounts are used by only one person. As to the second sentence, Defendants admit only that digital currency addresses need not be associated with particular individuals’ identifying information, but otherwise lack knowledge or information sufficient to admit or deny the second sentence, because the term “can’t be immediately traced to the person who uses it” is vague and undefined.
70. Defendants admit that Ethereum transactions appear on a public ledger, but otherwise lack knowledge and information sufficient to admit or deny the

first sentence, because the phrase “functionality depends” is vague and undefined. As to the second sentence, Defendants deny that Ethereum transactions are “visible to anyone,” but otherwise admit. As to the third sentence, Defendants admit only that transactions on the Ethereum blockchain cannot be erased from the public ledger, but otherwise lack knowledge and information sufficient to admit or deny the third sentence, because the phrase “hidden from view” is vague and undefined.

71. Defendants admit only that certain Ethereum transactions involve pseudonymous addresses, and that, in certain instances such addresses may be connected to their users, but otherwise deny. The second sentence is a legal conclusion to which no response is required, but to the extent one is deemed required, Defendants are without sufficient knowledge or information to admit or deny the second sentence, because the allegation does not identify the legal requirements to which the sentence refers. As to the third sentence, Defendants deny that “all of [a] user’s transactions and assets” can be inspected once their identity is connected to a digital currency address, but otherwise lack knowledge or information sufficient to admit or deny the allegations because the term “outsiders” and the phrase “address that he uses” are vague and undefined.

72. As to the first sentence of this paragraph, Defendants admit only that an

Ethereum user's transactions are generally visible on the Ethereum blockchain, but otherwise lack knowledge or information sufficient to admit or deny the allegations in the sentence because the terms "privacy tools" and "risks" are vague and undefined. The second sentence contains Plaintiffs' characterization of the cited article, to which no response is required. To the extent a response is deemed required, Defendants respectfully refer the Court to the cited article and deny that Plaintiffs' characterization is a complete and accurate statement of its contents. As to the third sentence, Defendants lack knowledge or information sufficient to admit or deny the allegations because the phrases "unwanted snooping" and "private relationships and intimate transactions" are vague and undefined.

73. This paragraph constitutes Plaintiffs' opinion, to which no response is required. To the extent a response is deemed required, Defendants admit only that Tornado Cash facilitates anonymous transactions by obfuscating their origin, destination, and counterparties, and otherwise lack knowledge or information sufficient to admit or deny the allegations in this paragraph, because it contains vague and undefined terms such as "where the Tornado Cash Tool comes in," "protect themselves from being followed in everything they do," "clear any discernable connection between their past transactions and their future transactions," and "new, apparently unconnected address."

74. As to the allegations in this paragraph, Defendants admit only that Tornado Cash facilitates anonymous transactions by obfuscating their origin, destination, and counterparties, and otherwise lack knowledge or information sufficient to admit or deny the allegations in this paragraph, because Defendants lack knowledge as what certain persons “will know,” “will see,” or “will [] move,” and because it contains vague and undefined terms such as “anyone attempting to track the user,” “outsider,” “Time 1,” “Time 2,” “Known User Address,” “control,” and “unrelated.”
75. The first sentence of this paragraph defines the scope of the Amended Complaint’s use of the phrase “Tornado Cash Tool,” and thus reflects Plaintiffs’ characterization of this action, so no response is required. To the extent a response is deemed required, Defendants admit that 29 addresses are listed in the Appendix to the Amended Complaint as “Challenged in this Lawsuit”, but otherwise lack knowledge sufficient to admit or deny the first sentence of this paragraph, because the phrase “core of the Tornado Cash Tool” is vague and undefined. As to the second sentence, Defendants admit only that the 29 addresses referenced as “Challenged in this Lawsuit” in the Appendix to the Amended Complaint correspond to fixed amounts of certain crypto assets, but otherwise lack knowledge or information regarding what “each user” will do sufficient to admit or deny the allegations in the second

sentence in this paragraph. As to the third sentence, Defendants deny that all transactions with the 29 addresses referenced in the first sentence are always indistinguishable, but otherwise lack knowledge or information sufficient to admit or deny the third sentence because the phrase “each interaction with any given address” is vague and undefined.

76. The allegations in this paragraph are denied.
77. Defendants admit only that Tornado Cash smart contracts do not lend or invest assets, and in that sense that they are “not like a bank,” but otherwise deny the allegations in the first sentence. The second sentence of this paragraph reflects Plaintiffs’ subjective opinion in the form of an analogy, to which no response is required. To the extent a response is deemed required, Defendants deny the allegations in the second sentence.
78. Denied.
79. The first sentence of this paragraph is denied. As to the second sentence, Defendants admit only that when Tornado Cash smart contract code receives instructions to run, such code generally runs, and otherwise deny. As to the third, fourth, and fifth sentences, Defendants admit only that code related to certain Tornado Cash smart contracts are designed to disallow future edits to their code, and otherwise deny the allegations in these sentences
80. This paragraph constitutes Plaintiffs’ opinion, to which no response is

required. To the extent a response is deemed required, Defendants lack knowledge or information sufficient to admit or deny the allegations.

81. This paragraph constitutes Plaintiffs' opinion, to which no response is required. To the extent a response is deemed required, Defendants lack knowledge or information sufficient to admit or deny the allegations in this paragraph, because it contains phrases that are vague and undefined, such as "private and secure," "widely regarded," "good practice," and "participate in Ethereum responsibly."
82. This paragraph constitutes Plaintiffs' opinion, to which no response is required. To the extent a response is deemed required, Defendants admit, with respect to the second sentence, only that Tornado Cash facilitates anonymous transactions by obfuscating their origin, destination, and counterparties. Defendants otherwise lack knowledge or information sufficient to admit or deny the allegations in this paragraph, because it contains numerous phrases that are vague and undefined.
83. This paragraph constitutes Plaintiffs' opinion, to which no response is required. To the extent a response is deemed required, Defendants lack knowledge or information sufficient to admit or deny the allegations in this paragraph, because it contains numerous phrases that are vague and undefined, such as "for some time," "widely believed," "lead the way,"

“other crypto assets,” and “many American governors.” Defendants respectfully refer the Court to the cited articles for a complete and accurate statement of their contents, and deny any aspects of Plaintiffs allegations that incorrectly characterize the articles cited.

84. This paragraph constitutes Plaintiffs’ opinion, to which no response is required. To the extent a response is deemed required, Defendants lack knowledge or information sufficient to admit or deny the allegations because it contains phrases that are vague and undefined, such as “America’s leading role has been thrown into reverse,” “punish crypto users,” and “hyper-regulate.” Defendants respectfully refer the Court to the cited articles for a complete and accurate statement of their contents, and deny any aspects of Plaintiffs allegations that incorrectly characterize the articles cited.
85. This paragraph constitutes Plaintiffs’ opinion, to which no response is required. To the extent a response is deemed required, Defendants deny the allegations in this paragraph.
86. This paragraph contains Plaintiffs’ characterization of IEEPA, to which no response is required. To the extent a response is deemed required, Defendants admit that the quoted language appears in the statute, but otherwise respectfully refer the Court to the statute and deny that Plaintiffs’ characterization is a complete and accurate statement of its contents.

87. This paragraph contains Plaintiffs' characterization of IEEPA, to which no response is required. To the extent a response is deemed required, Defendants admit that the quoted language appears in the statute, but otherwise respectfully refer the Court to the statute and deny that Plaintiffs' characterization is a complete and accurate statement of its contents.
88. This paragraph contains Plaintiffs' characterization of IEEPA, to which no response is required. To the extent a response is deemed required, Defendants admit that the quoted language appears in the statute, but otherwise respectfully refer the Court to the statute and deny that Plaintiffs' characterization is a complete and accurate statement of its contents.
89. This paragraph contains Plaintiffs' characterization of IEEPA, to which no response is required. To the extent a response is deemed required, Defendants admit that the quoted language appears in the statute, but otherwise respectfully refer the Court to the statute and deny that Plaintiffs' characterization is a complete and accurate statement of its contents.
90. This paragraph contains Plaintiffs' characterization of the North Korea Sanctions and Policy Enhancement Act, to which no response is required. To the extent a response is deemed required, Defendants admit that the quoted language appears in the statute, but otherwise respectfully refer the Court to the statute and deny that Plaintiffs' characterization is a complete

and accurate statement of its contents.

91. This paragraph consists of Plaintiffs' characterization of the cited Executive orders, to which no response is required. To the extent a response is deemed required, Defendants admit only that the quoted language appears in the cited Executive orders, but otherwise respectfully refer the Court to the Executive orders and deny that Plaintiffs' characterization is a complete and accurate statement of their contents.
92. This paragraph contains Plaintiffs' characterization of OFAC regulations, to which no response is required. To the extent a response is deemed required, Defendants respectfully refer the Court to the regulations and deny that Plaintiffs' characterization is a complete and accurate statement of their contents.
93. This paragraph contains Plaintiffs' characterization of OFAC regulations, to which no response is required. To the extent a response is deemed required, Defendants admit that the quoted language appears in the regulations, but otherwise respectfully refer the Court to the regulations and deny that Plaintiffs' characterization is a complete and accurate statement of their contents. Defendants deny that the "Tornado Cash Tool was criminalized," or that the challenged actions constituted "criminalization . . . and re-criminalization."

94. The first sentence of this paragraph contains Plaintiffs' characterization of OFAC regulations, to which no response is required. To the extent a response is deemed required, Defendants admit that the quoted language appears in the regulations, but otherwise respectfully refer the Court to the regulations and deny that Plaintiffs' characterization is a complete and accurate statement of their contents. As to the second sentence, it is a legal conclusion to which no response is required. To the extent a response is deemed required, Defendants admit only that the terms "idea," "tool," and "technology" are not contained within the cited regulation, but otherwise deny the allegations in this sentence.
95. Defendants admit only that OFAC publishes the SDN List, which includes the names and other identifying information of persons whose property and interests in property are blocked to the extent they are within the United States or within the possession or control of U.S. persons. Defendants otherwise deny the allegations in this paragraph.
96. Defendants deny the first sentence of the paragraph. The remainder of this paragraph contains Plaintiffs' characterization of OFAC regulations, to which no response is required. To the extent a response is deemed required, Defendants respectfully refer the Court to the regulations and deny that Plaintiffs' characterization is a complete and accurate statement of their

contents.

97. Admitted.

98. Defendants admit only that a U.S. person who willfully engages in a transaction or transactions with a designated person has committed a felony offense, unless such transaction or transactions are authorized or exempt from applicable OFAC regulations, but otherwise deny.

99. As to the first sentence of this paragraph, Defendants admit only that on August 8, 2022, OFAC added Tornado Cash to the SDN List. The remainder of the first sentence reflects Plaintiffs' opinion, to which no response is required. To the extent a response is deemed required, Defendants deny the remaining allegations in the first sentence. As to the second sentence, Defendants admit only that its August 8 designation identified 38 Ethereum addresses, and otherwise deny.

100. The first sentence of this paragraph reflects Plaintiffs' opinion, to which no response is required. To the extent a response is deemed required, Defendants deny the allegations. As to the second sentence, Defendants admit that the quoted language appears in the August 8, 2022 press release, but otherwise deny the allegations, and respectfully refer the Court to the press release for a complete and accurate statement of its contents.

101. The allegations in this paragraph consist of Plaintiffs' characterization of this

action and Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants deny that Plaintiffs are entitled to any relief, or that Defendants have violated any of the cited authorities.

102. As to the first sentence of this paragraph, Defendants admit only that on November 8, 2022, OFAC withdrew the August 8, 2022 designation of Tornado Cash, and otherwise deny. As to the second sentence Defendants deny that the November 8 action constituted "re-criminaliz[ing]," and as to the remainder of the sentence, admit only that on November 8, 2022, OFAC delisted and simultaneously redesignated Tornado Cash under Executive Orders 13722 and 13694, and that the redesignation took into account additional information and included an additional basis for the designation of Tornado Cash regarding its support for DPRK activities, and otherwise deny the allegations in the second sentence. The third sentence contains Plaintiffs' characterization of Treasury's November 8, 2022 press release, to which no response is required. To the extent a response is deemed required, Defendants respectfully refer the Court to the press release and deny that Plaintiffs' characterization is a complete and accurate statement of its contents.

103. This paragraph contains Plaintiffs' characterization of Treasury's November

8, 2022 press release, to which no response is required. To the extent a response is deemed required, Defendants admit that the quoted language appears in OFAC's press release, but respectfully refer the Court to the press release and deny that Plaintiffs' characterization is a complete and accurate statement of its contents.

104. As to the first sentence of this paragraph, Defendants admit that the quoted word "person" appears in FAQ 1095, but otherwise deny. As to the second and third sentences, Defendants admit that on November 8, 2022, OFAC published the linked FAQ addressing the Tornado Cash designation, and admit that the quoted language appears in the FAQ, but otherwise respectfully refer the Court to the FAQ itself, and deny that Plaintiffs' characterization is a complete and accurate statement of their contents.
105. Defendants admit only that OFAC identified 90 digital currency addresses in connection with the November 8, 2022 SDN List entry for Tornado Cash. The allegations in this paragraph are otherwise denied.
106. The first sentence of this paragraph consists of Plaintiffs' characterization of this action, to which no response is required. To the extent a response is deemed required, Defendants admit only that the 29 digital currency addresses identified in the appendix to the Amended Complaint were identified in connection with the November 8, 2022 designation of Tornado

Cash. As to the second sentence, Defendants lack knowledge or information sufficient to admit or deny the allegations because “host the technology and support functions that together constitute the core of the Tornado Cash Tool,” is vague and undefined. As to the third sentence, Defendants admit only that 29 digital currency addresses are listed in the appendix to the Amended Complaint as “Challenged in this Lawsuit,” and otherwise deny. The fourth sentence is denied.

107. Defendants admit that there are 61 addresses listed in the appendix to the Amended complaint as “Not Challenged in this Lawsuit,” but otherwise lack knowledge or information sufficient to admit or deny the allegations because the terms “non-functional,” “serve other purposes,” and “controlled by someone” are vague and undefined.
108. This paragraph consists of Plaintiffs’ characterization of this action, and legal conclusions regarding Defendants’ positions, to which no response is required. To the extent a response is deemed required, Defendants respond as follows: With respect to the first sentence, Defendants admit only that 61 Ethereum addresses are listed in the appendix to the amended complaint as “Not Challenged in this Lawsuit,” and otherwise respectfully refer the court to the designation itself for a complete and accurate reflection of its contents, and deny the remaining allegations in this sentence. With respect to the

second sentence, Defendants respectfully refer the Court to FAQ 1095 for a full and accurate reflection of its contents, and otherwise deny the allegations in this sentence. With respect to the third sentence, Defendants admit only that 29 addresses are listed in the appendix to the Amended Complaint as “Challenged in this Action,” and otherwise deny the allegations in this sentence.

109. Defendants admit the first sentence of this paragraph. As to the second sentence, Defendants admit, but clarify that Tornado Cash has functionality to operate on blockchains other than the Ethereum blockchain. The third sentence consists of Plaintiffs’ characterization of the August 8 and November 8, 2022 designations and Plaintiffs’ legal argument and legal conclusions regarding those and hypothetical future designations, to which no response is required. To the extent a response is deemed required, Defendants respectfully refer the court to the designations for a complete and accurate reflection of their contents, and otherwise deny the allegations. *See* Cyber-related Designation (Aug. 8, 2022) <https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20220808>; Burma-related Designations; North Korea Designations; Cyber-related Designation; Cyber-related Designation Removal; Publication of Cyber-related Frequently Asked Questions (Nov. 8, 2022); *see also* 87 Fed. Reg. 49,652 (Aug. 11, 2022); 87

Fed. Reg. 68,578 (Nov. 15, 2022).

110. As to the first sentence of this paragraph, Defendants admit only that certain of the addresses identified in the Appendix to the Amended Complaint as “Challenged in this Lawsuit” are designed to disallow future edits to their code, but otherwise lack knowledge or information sufficient to admit or deny the allegations. The remaining sentences consist of legal conclusions to which no response is required, but to the extent a response is deemed required, Defendants deny the allegations in those sentences.
111. This paragraph consists of Plaintiffs’ legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants deny the allegations in this paragraph.
112. This paragraph consists of Plaintiffs’ legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants deny the allegations in this paragraph. Defendants respectfully refer the court to the cited FAQ and press article for a complete and accurate reflection of their contents.
113. This paragraph consists of Plaintiffs’ legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants deny the allegations in this paragraph. Defendants respectfully refer the court to the cited FAQ for a complete and accurate

reflection of its contents.

114. The first and second sentences of this paragraph are denied. The third sentence consists of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants deny.
115. This paragraph appears to consist of Plaintiffs' characterization of Treasury's August 8, 2022 press release. Defendants respectfully refer the court to the press release for a complete and accurate reflection of its contents, and deny any allegations that are inconsistent with it. See Treasury Sanctions North Korean Senior Officials and Entities Associated with Human Rights Abuses (July 6, 2016) home.treasury.gov/news/press-releases/jl0506.
116. This paragraph appears to consist of Plaintiffs' characterization of OFAC's FAQ 1095 (last updated Nov. 8, 2022), <https://home.treasury.gov/policy-issues/financial-sanctions/faqs/1095>. Defendants respectfully refer the court to the FAQ for a complete and accurate reflection of its contents, and deny any allegations that are inconsistent with it.
117. Denied.
118. The first sentence of this paragraph consists of Plaintiffs' characterization of this action and Plaintiffs' opinion, to which no response is required. To the extent a response is deemed required, Defendants deny. Defendants lack

knowledge sufficient to admit or deny the second sentence, because the terms “good tools” and “bad people” are vague and undefined. The third sentence consists of Plaintiffs’ legal argument, legal conclusions, and opinion, to which no response is required. To the extent a response is deemed required, Defendants deny.

119. This paragraph consists of Plaintiffs’ legal argument, legal conclusions, and opinion, to which no response is required. To the extent a response is deemed required, Defendants deny.

120. The first sentence of this paragraph consists of Plaintiffs’ legal argument, legal conclusions, and opinion, to which no response is required. To the extent a response is deemed required, Defendants deny. As to the second sentence, Defendants admit only that certain Tornado Cash smart contracts remain online and operable, and otherwise deny.

121. The first sentence of this paragraph consists of Plaintiffs’ opinion and legal argument, to which no response is required. To the extent a response is deemed required, Defendants deny. As to the second sentence, Defendants admit only that certain Tornado Cash smart contracts are still operational, but otherwise deny. As to the third sentence, Defendants admit only that individuals may receive unsolicited crypto assets sent through Tornado Cash, *see* FAQ 1078 (last updated Nov. 8, 2022), <https://home.treasury.gov/policy->

[issues/financial-sanctions/faqs/added/2022-09-13](#), but otherwise deny the allegations in that sentence. As to the fourth sentence, Defendants admit only that when a U.S. person receives assets from a person named on the SDN List, in general such assets must be blocked and reported to OFAC. Defendants otherwise deny the allegations in the fourth sentence.

122. This paragraph contains Plaintiffs' characterization of the cited article, to which no response is required. To the extent a response is deemed required, Defendants respectfully refer the Court to the cited article and deny that Plaintiffs' characterization is a complete and accurate statement of its contents.
123. This paragraph contains Plaintiffs' characterization of the cited articles, to which no response is required. To the extent a response is deemed required, Defendants respectfully refer the Court to the cited articles and deny that Plaintiffs' characterization is a complete and accurate statement of their contents.
124. The first sentence of this paragraph consists of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants admit only that OFAC reporting obligations may apply to U.S. persons who have received unsolicited and nominal amounts of virtual currency or other virtual assets from Tornado Cash smart

contracts, but otherwise deny the allegations. The remainder of this paragraph contains Plaintiffs' characterization of FAQ No. 1078, to which no response is required. To the extent a response is deemed required, Defendants respectfully refer the Court to the FAQ and deny that Plaintiffs' characterization is a complete and accurate statement of its contents.

125. This paragraph consists of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants deny the allegations and deny that Plaintiffs are entitled to any relief.
126. This paragraph consists of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants deny the allegations and deny that Plaintiffs are entitled to any relief.
127. This paragraph consists of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants deny the allegations and deny that Plaintiffs are entitled to any relief.
128. Defendants hereby incorporate their responses to all preceding paragraphs of the Amended Complaint by reference.
129. This paragraph contains Plaintiffs' characterization of IEEPA, to which no

response is required. To the extent a response is deemed required, Defendants admit that the quoted language appears in the statute, but otherwise respectfully refer the Court to the statute and deny that Plaintiffs' characterization is a complete and accurate statement of its contents.

130. This paragraph contains Plaintiffs' characterization of the North Korea Sanctions and Policy Enhancement Act, to which no response is required. To the extent a response is deemed required, Defendants admit that the quoted language appears in 22 U.S.C. §9214 and 50 U.S.C. §1702, but otherwise respectfully refer the Court to the statute and deny that Plaintiffs' characterization is a complete and accurate statement of its contents.
131. This paragraph consists of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants deny.
132. The first and second sentences of this paragraph reflect Plaintiffs' opinion, to which no response is required, and include phrases such as "[m]any uses" and "[m]any involve," which are vague and undefined. Thus, Defendants lack knowledge or information sufficient to admit or deny the allegations in the first and second sentences. The third sentence is denied.
133. This paragraph consists of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response is deemed

required, Defendants deny.

134. This paragraph consists of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants admit only that the quoted language appears in the cited statute, but otherwise deny, and respectfully refer the Court to the cited statute for a complete and accurate statement of its contents.
135. Defendants hereby incorporate their responses to all preceding paragraphs of the Amended Complaint by reference.
136. This paragraph consists of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants admit only that the quoted language appears in the cited Executive orders and regulation, but otherwise respectfully refer the Court to the Executive orders and regulation and deny that Plaintiffs' characterization is a complete and accurate statement of their contents.
137. The first sentence of this paragraph consists of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants admit only that the quoted language appears in the cited regulations, but otherwise respectfully refer the Court to the regulations and deny that Plaintiffs' characterization is a complete and accurate statement of their contents. As to the second sentence, it is a legal

conclusion to which no response is required. To the extent a response is deemed required, Defendants admit only that the terms “idea,” “tool,” and “technology” are not contained within the cited regulation, but otherwise deny the allegations in this sentence.

138. This paragraph consists of legal conclusions and Plaintiffs’ characterization of Defendants’ August 8, 2022 and November 8, 2022 press release, to which no response is required. To the extent a response is deemed required, Defendants admit that the quoted language appears in the press releases, but otherwise deny the allegations, and respectfully refer the Court to the press release for a complete and accurate statement of its contents.
139. This paragraph consists of Plaintiffs’ legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants admit that none of the 29 addresses listed as “Challenged in this Lawsuit” in the appendix to the Amended Complaint are a person. The second sentence is denied.
140. This paragraph consists of Plaintiffs’ legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants admit only that the quoted language appears in the cited statute, but otherwise deny, and respectfully refer the Court to the statute for a complete and accurate statement of its contents.

141. Defendants hereby incorporate their responses to all preceding paragraphs of the Amended Complaint by reference.
142. This paragraph consists of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants admit that the quoted language appears in the cited case, but otherwise deny.
143. This paragraph consists of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants deny.
144. This paragraph consists of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants deny.
145. This paragraph consists of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants deny.
146. This paragraph consists of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants deny.
147. This paragraph consists of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response is deemed

required, Defendants deny, and respectfully refer the Court to the cited regulations and website for a complete and accurate statement of their contents.

148. This first sentence of this paragraph consists of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants deny. The second and third sentences consist of Plaintiffs' characterization of the August 8, 2022 and November 8, 2022 press releases, to which no response is required. To the extent a response is deemed required, Defendants admit only that the quoted language appears in the cited press releases, but otherwise respectfully refer the Court to the press releases and deny that Plaintiffs' characterization is a complete and accurate statement of their contents.
149. This first sentence of this paragraph consists of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants deny.
150. This paragraph consists of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants deny.
151. This first sentence of this paragraph consists of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response

is deemed required, Defendants admit only that the quoted language appears in the cited regulations, but otherwise respectfully refer the Court to the regulations and deny that Plaintiffs' characterization is a complete and accurate statement of their contents. The second sentence consists of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants deny.

152. This paragraph consists of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants deny.

153. Defendants hereby incorporate their responses to all preceding paragraphs of the Amended Complaint by reference.

154. This paragraph consists of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants deny.

155. This paragraph consists of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants admit that the quoted language appears in the cited cases, but otherwise deny.

156. This paragraph consists of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response is deemed

required, Defendants deny.

157. This paragraph consists of Plaintiffs' legal argument and legal conclusions, to which no response is required. To the extent a response is deemed required, Defendants admit only that the quoted language appears in the cited statute, but otherwise deny the allegations, and respectfully refer the Court to the statute for a complete and accurate statement of its contents.

The remaining unnumbered paragraphs constitute a prayer for relief to which no response is required. To the extent a response is deemed required, Defendants deny that Plaintiffs are entitled to the relief requested, or to any relief whatsoever.

Defendants hereby deny all allegations in Plaintiffs' Amended Complaint not expressly admitted or denied.

The Appendix to the Amended Complaint constitutes Plaintiffs' characterization of this action, to which no response is required, but to the extent a response is deemed required, Defendants deny that the list constitutes "Sanctioned Addresses." As to the allegation that the 29 addresses listed as "Challenged in this Lawsuit" are "Immutable," Defendants admit only that certain of the addresses identified in the Appendix to the Amended Complaint as "Challenged in this Lawsuit" are designed to disallow future edits to their code, but otherwise lack knowledge or information sufficient to admit or deny the allegations.

Affirmative Defenses

- A. Plaintiffs lack standing to bring this lawsuit.
- B. Plaintiffs fail to state claims for which relief can be granted.
- C. Defendants at all relevant times acted in accordance with applicable legal authority, and did not violate the Constitution, Administrative Procedure Act, IEEPA, the United Nations Participations Act of 1945, North Korea Sanctions and Policy Enhancement Act of 2016, or any other applicable statute or authority.
- D. To the extent that Plaintiff's claims rely on constitutionally protected interests or applicable case law, such authorities do not apply to the circumstances alleged by Plaintiffs.

Wherefore, having fully Answered, Defendants respectfully request that the Court enter judgment dismissing this action with prejudice and awarding Defendants costs and other such relief as the Court may deem appropriate.

Dated: January 9, 2022

Respectfully submitted,

BRIAN M. BOYNTON
Principal Deputy Assistant Attorney
General

ALEXANDER K. HAAS
Director

DIANE KELLEHER
Assistant Director

STEPHEN M. ELLIOTT
Senior Counsel

CHRISTOPHER R. HEALY
/s/ Christine L. Coogle
CHRISTINE L. COOGLE
Trial Attorneys
Federal Programs Branch
Civil Division
United States Department of Justice
1100 L St. NW
Washington, D.C. 20005
202-880-0282
christine.l.coogle@usdoj.gov

Counsel for Defendants

TAB 36

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF FLORIDA
PENSACOLA DIVISION**

COIN CENTER; PATRICK
O’SULLIVAN; JOHN DOE; and
DAVID HOFFMAN,
Plaintiffs,

v.

JANET YELLEN, in her official
capacity as Secretary of the Treasury;
DEPARTMENT OF THE
TREASURY; ANDREA M. GACKI,
in her official capacity as Director of
the Office of Foreign Assets Control;
and OFFICE OF FOREIGN
ASSETS CONTROL,
Defendants.

Case No.
3:22-cv-20375-TKW-ZCB

PLAINTIFFS’ MOTION FOR SUMMARY JUDGMENT

Pursuant to Federal Rule of Civil Procedure 56, Plaintiffs respectfully move for summary judgment against Defendants. For the reasons explained in the accompanying memorandum, Defendants’ criminalization of all transactions involving the “Tornado Cash” software tool, as it resides at the 29 challenged Ethereum addresses, exceeded their statutory authority and was contrary to law, was arbitrary and capricious, and violated the First Amendment. Plaintiffs respectfully request that the Court enter summary judgment for Plaintiffs and hold unlawful and set aside the criminalization of transactions involving the 29 challenged addresses.

Oral Argument Statement. Pursuant to Local Rule 7.1(K), Plaintiffs respectfully request oral argument on this motion. The motion raises important questions about the executive's power over domestic affairs under the International Emergency Economic Power Act, and argument would aid the Court in answering those questions. Plaintiffs estimate that one hour for argument would be appropriate.

Dated: May 26, 2023

Respectfully submitted,

Michael A. Sasso
Florida Bar No. 93814
masasso@sasso-law.com
Christian Bonta
Florida Bar No. 1010347
cbonta@sasso-law.com
SASSO & SASSO, P.A.
1031 West Morse Blvd, Suite 120
Winter Park, Florida 32789
Tel.: (407) 644-7161

s/Cameron T. Norris
Jeffrey M. Harris*
Cameron T. Norris*
Jeffrey S. Hetzel*
CONSOVOY MCCARTHY PLLC
1600 Wilson Boulevard, Suite 700
Arlington, VA 22209
Telephone: 703.243.9423

J. Abraham Sutherland*
106 Connally Street
Black Mountain, NC 28711
Telephone: 805.689.4577.

*pro hac vice

Counsel for Plaintiffs

CERTIFICATE OF SERVICE

I e-filed this motion with the Court on May 26, 2023, which emailed everyone requiring notice.

/s/ Cameron T. Norris
Counsel for Plaintiffs

CERTIFICATE OF COMPLIANCE

I also certify that this memorandum contains 146 words, excluding the parts that may be excluded.

/s/ Cameron T. Norris
Counsel for Plaintiffs

Exhibit A

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF FLORIDA
PENSACOLA DIVISION**

COIN CENTER; PATRICK
O’SULLIVAN; JOHN DOE; and
DAVID HOFFMAN,

Plaintiffs,

v.

JANET YELLEN, in her official
capacity as Secretary of the Treasury;
DEPARTMENT OF THE
TREASURY; ANDREA M. GACKI,
in her official capacity as Director of
the Office of Foreign Assets Control;
and OFFICE OF FOREIGN ASSETS
CONTROL,

Defendants.

Case No.

3:22-cv-20375-TKW-ZCB

DECLARATION OF PATRICK O’SULLIVAN

I, Patrick O’Sullivan, in accordance with 28 U.S.C. § 1746, declare as follows:

1. I am over eighteen years old and competent to sign this declaration.

These statements are based on my personal knowledge.

2. I live in Santa Rosa County, Florida and work as a software developer. At the time of the filing of the complaints in this case, I lived in Escambia County, Florida.

3. I am an American citizen.

4. I am routinely paid by my employer in crypto assets. As a result, my employer and those who know my employer’s Ethereum address, such as other employees and other businesses, can identify my cryptocurrency address on the Ethereum public ledger. That can allow them to track my salary, my assets, and my unrelated personal activities. I would like to keep those things private.

5. I also use crypto assets in other ways that could allow third parties to identify my cryptocurrency address on the Ethereum public ledger and to track my salary, my assets, and my unrelated personal activities. I would like to keep those things private.

6. I am a publicly known user and developer of Ethereum-related technology. As a result, I am at increased risk of having my activities monitored, which can imperil my and my family’s privacy and personal safety.

7. I therefore routinely use cryptocurrency privacy tools to protect myself and my family.

8. One of the most important privacy tools for Ethereum users is the “Tornado Cash” tool, or the core software tool at issue in this case.

9. If not for the criminalization of the tool, I would use it to protect my privacy.

10. Specifically, I would deposit my crypto assets from my publicly known address to one of the core software tool addresses. I would then withdraw my crypto asset from that address to a new, more private address under my control.

11. I would not use a registered relay. I believe that registered relayers are optional and unnecessary to achieving my goals of improving my privacy. I do not wish to use them and would not use them.

12. My use would therefore consist of my public address sending my crypto asset, such as 0.1 ETH, then my private address withdrawing that same 0.1 ETH, without any payment to any registered relay:

[0.1 ETH] [my more public address] → 0x12D66f87...

[0.1 ETH] 0x12D66f87... → [my more private address]


13. Throughout the entirety of this transaction, nothing would be sent to a registered relay, software writer, or DAO member. The only payment that I would make would be the standard Ethereum transaction fee associated with any transaction.

14. Throughout my planned transactions, I alone would control the funds. And I alone would have access to both the public and private address.

15. Because of Defendants' criminalization I am prohibited from undertaking my planned course of activity and impeded from protecting my privacy.

16. I declare under penalty of perjury that the foregoing is true and correct.

Executed May 25, 2023 in Santa Rosa County, Florida.

A handwritten signature in cursive script, reading "Pat O'Sullivan". The signature is written in black ink and is positioned above a horizontal line.

Patrick O'Sullivan

Exhibit B

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF FLORIDA
PENSACOLA DIVISION**

COIN CENTER; PATRICK
O’SULLIVAN; JOHN DOE; and
DAVID HOFFMAN,

Plaintiffs,

v.

JANET YELLEN, in her official
capacity as Secretary of the Treasury;
DEPARTMENT OF THE
TREASURY; ANDREA M. GACKI,
in her official capacity as Director of
the Office of Foreign Assets Control;
and OFFICE OF FOREIGN ASSETS
CONTROL,

Defendants.

Case No.

3:22-cv-20375-TKW-ZCB

DECLARATION OF JOHN DOE

I, John Doe, in accordance with 28 U.S.C. § 1746, declare as follows:

1. I am over eighteen years old and competent to sign this declaration.

These statements are based on my personal knowledge.

2. I live in Georgia and am a human-rights advocate.

3. I am an American citizen.

4. I am proceeding pseudonymously because I believe that, if my identity is exposed, Russian agents will learn about my role in pro-Ukrainian activities and could harm me and my family.

5. After Russia invaded Ukraine, I began providing and coordinating support for Ukrainians under attack. Since April 2022, I supported Ukrainians personally and facilitated sizable crypto donations from other donors. I and my donors call ourselves the 688th Support Brigade.

6. I made and facilitated sizable donations that went to supporting the most urgent needs of Ukrainians at war. My efforts have paid for gloves, shoes, helmets, drones, and vehicles to assist Ukrainian frontline efforts.

7. Crypto donations to Ukraine have made a substantial positive impact.

8. I and the donors I help came to the mutual agreement that donating to Ukrainians could jeopardize our and our families' safety. Without privacy protections, Russian agents and Russian-funded hackers could identify and retaliate against donors like us for providing frontline aid. If our identities were revealed, our lives could be in danger when we travel abroad and we could be targeted by hackers. We want to

support Ukraine without fear of being harmed. We also value making contributions privately.

9. Every single donor has used the “Tornado Cash” tool, or the core software tool at issue in this case, to achieve that privacy. Under my direction, a donor will move her crypto asset to a tool address, then later withdraw it from that address to an account controlled exclusively by me for the provision of aid. From that latter account, I can send the assets to recipients who purchase the aid for Ukraine. An outside observer cannot tell whose assets are being sent to the latter account because they all come through an address with this privacy tool.

10. I myself have contributed to these efforts using the software tool. I have deposited assets from a personal address to a tool address, and then withdrawn those assets from that address to my address that I use exclusively for the provision of aid.

11. As a result of Defendants’ criminalization, our donations have stopped. I am not comfortable facilitating donations without the protection of the tool. I am not confident that any alternative methods will provide a sufficient level of privacy or security.

12. We now no longer donate to the cause we wish to support.

13. If not for the criminalization of the tool, I and my donors would have continued to use it and to provide aid. We do not need to use registered relayers and would not use them. Instead, we would deposit funds from our more public addresses and then withdraw them to a pre-funded address. In cases where a donor would like a

new pre-funded address, I would send a small amount of funds to a donor's new and private address from the donation address I control. After the donor withdraws their funds to that address, the donor would complete the donation by sending the funds to the donation address I control. As in the past, I would then direct the aid from that account to recipients who can purchase goods for Ukraine.

14. Throughout the entirety of these transactions, nothing would be sent to a registered relayer, software writer, or DAO member. The only payment that we would make would be the standard Ethereum transaction fee associated with any transaction.

15. Because of Defendants' criminalization, we are prohibited from undertaking our planned course of activity and from contributing, in privacy, to the causes that we believe in.

16. I declare under penalty of perjury that the foregoing is true and correct.

Executed May 25, 2023 in Georgia.

John Doe

John Doe

Exhibit C

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF FLORIDA
PENSACOLA DIVISION**

COIN CENTER; PATRICK
O’SULLIVAN; JOHN DOE; and
DAVID HOFFMAN,

Plaintiffs,

v.

JANET YELLEN, in her official
capacity as Secretary of the Treasury;
DEPARTMENT OF THE
TREASURY; ANDREA M. GACKI,
in her official capacity as Director of
the Office of Foreign Assets Control;
and OFFICE OF FOREIGN ASSETS
CONTROL,

Defendants.

Case No.

3:22-cv-20375-TKW-ZCB

DECLARATION OF DAVID HOFFMAN

I, David Hoffman, in accordance with 28 U.S.C. § 1746, declare as follows:

1. I am over eighteen years old and competent to sign this declaration.

These statements are based on my personal knowledge.

2. I live in New York and work as a crypto asset investor and entrepreneur.

3. I am an American citizen.

4. I use Ethereum publicly. I make one of my Ethereum addresses public, so that anyone can access it online and transact with me.

5. Because I make one of my Ethereum addresses public, anyone can send assets to it without my knowledge or consent. After Defendants criminalized the “Tornado Cash” tool, or the core software tool at issue in this case, someone sent crypto assets to me through the tool.

6. The burdens of potential liability and reporting obligations were forced upon me because I received payment through one of the listed addresses. I am under continuing threat of being subjected to the same burdens by future senders, any one of whom can route a payment to my public address through the tool.

7. Also because I make one of my Ethereum addresses public, third parties can identify my activities on the Ethereum public ledger. That can allow them to track my salary, my assets, and my unrelated personal activities. I would like to keep some of those things private.

8. I therefore routinely use cryptocurrency privacy tools to protect myself.

9. One of the most important privacy tools for Ethereum users is the core software tool at issue in this case.

10. If not for the criminalization of the tool, I would use it to protect my privacy.

11. Specifically, I would deposit my crypto assets from my publicly known address to one of the core software tool addresses. I would then withdraw my crypto asset from that address to a new, more private address under my control.

12. I would not use a registered relay. I believe that registered relayers are optional and unnecessary to achieving my goals of improving my privacy. I do not wish to use them and would not use them.

13. My use would therefore consist of my public address sending my crypto asset, such as 0.1 ETH, then my private address withdrawing that same 0.1 ETH, without any payment to any registered relay:

[0.1 ETH] [my more public address] → 0x12D66f87...

[0.1 ETH] 0x12D66f87... → [my more private address]

14. Throughout the entirety of this transaction, nothing would be sent to a registered relay, software writer, or DAO member. The only payment that I would make would be the standard Ethereum transaction fee associated with any transaction.

15. Throughout my planned transaction, I alone would control the funds. And I alone would have access to both the public and private address.

16. Because of Defendants' criminalization I am prohibited from undertaking my planned course of activity and impeded from protecting my privacy.

17. I declare under penalty of perjury that the foregoing is true and correct.

Executed May 25, 2023 in New York.

A handwritten signature in black ink, appearing to read "David Hoffman", written over a horizontal line.

David Hoffman

Exhibit D

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF FLORIDA
PENSACOLA DIVISION**

COIN CENTER; PATRICK
O'SULLIVAN; JOHN DOE; and
DAVID HOFFMAN,

Plaintiffs,

v.

JANET YELLEN, in her official
capacity as Secretary of the Treasury;
DEPARTMENT OF THE
TREASURY; ANDREA M. GACKI,
in her official capacity as Director of
the Office of Foreign Assets Control;
and OFFICE OF FOREIGN ASSETS
CONTROL,

Defendants.

Case No.

3:22-cv-20375-TKW-ZCB

**DECLARATION OF JERRY BRITO,
EXECUTIVE DIRECTOR OF COIN CENTER**

I, Jerry Brito, in accordance with 28 U.S.C. § 1746, declare as follows:

1. I am over eighteen years old and competent to sign this declaration.

These statements are based on my personal knowledge.

2. I am the Executive Director of Coin Center and have been since 2014.

3. Coin Center is the leading nonprofit research and advocacy center focused on the public-policy issues facing cryptocurrency and decentralized computing technologies. We defend the rights of individuals to build and use free and open cryptocurrency networks, including the right to write and publish code, the right to assemble into peer-to-peer networks, and the right to do all this privately. Coin Center produces and publishes research, educates policymakers and the media about cryptocurrencies, advocates for sound public policy, and defends digital civil liberties.

4. Coin Center is based in Washington, D.C.

5. Coin Center uses Ethereum. We routinely receive contributions from donors in the form of crypto assets.

6. Some of Coin Center's donors want to keep their contribution and their other personal financial activities private.

7. Coin Center's donors therefore used in the past, and would likely use in the future, the "Tornado Cash" tool at issue in this lawsuit to protect their privacy.

8. In the past, our donors have deposited a crypto asset to a tool address, then withdrawn it to a more private address, then sent the asset to Coin Center. Third

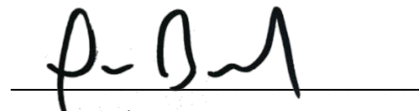
parties can't tell whose assets are being sent to Coin Center's account when they come this way, so their donations remain private.

9. We are aware of donations that passed through the tool without the use of registered relayers, but are not aware of any donations that used registered relayers. Future donors would not need to use a registered relayer to donate to us privately. We do not intend to use registered relayers if we use the tool.

10. As a result of Defendants' criminalization of the tool, our donors are impeded from engaging in expressive advocacy privately. Coin Center is likely to lose contributions from our donors who wish to remain private.

11. I declare under penalty of perjury that the foregoing is true and correct.

Executed May 25, 2023 in Washington, D.C.

A handwritten signature in black ink, appearing to read "J. Brito", is written over a horizontal line.

Jerry Brito

Executive Director, Coin Center

TAB 68

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF FLORIDA
PENSACOLA DIVISION**

COIN CENTER; PATRICK O’SUL-
LIVAN; JOHN DOE; and DAVID
HOFFMAN,

Plaintiffs,

v.

JANET YELLEN, in her official ca-
pacity as Secretary of the Treasury;
DEPARTMENT OF THE TREAS-
URY; ANDREA M. GACKI, in her
official capacity as Director of the Of-
fice of Foreign Assets Control; and
OFFICE OF FOREIGN ASSETS
CONTROL,

Defendants.

Case No.

3:22-cv-20375-TKW-ZCB

**JOINT APPENDIX OF ADMINISTRATIVE RECORD DOCUMENTS
CITED IN PARTIES’ CROSS-MOTIONS FOR SUMMARY JUDGMENT**

The parties respectfully submit this joint appendix containing the administrative record documents cited in their summary-judgment briefs. The joint appendix contains the following documents from the administrative record:

Administrative Record Document	Administrative Record Citation
Volume I	
Designation and Blocking Memorandum	A.R. 1-5
Press Release	A.R. 9-12
Evidentiary Memorandum	A.R. 13-100
Exhibit 6: CoinDesk, <i>Tornado Cash Co-Founder Says the Mixer Protocol is Unstoppable</i>	A.R. 137-149
Exhibit 7: Decrypt.co, <i>Tornado Cash Ethereum Token Down 50% After Sanctions</i>	A.R. 150-157
Exhibit 15: Medium, <i>Tornado Cash Introduces Arbitrary Amounts & Shielded Transfers</i>	A.R. 184-189
Exhibit 54: Department of the Treasury, <i>Treasury Takes Robust Actions to Counter Ransomware</i>	A.R. 474-479
Exhibit 58: Ethereum, <i>Ethereum Accounts</i>	A.R. 505-513
Exhibit 59: Chainalysis, <i>Dissecting the DAO: Web3 Ownership is Surprisingly Complicated</i>	A.R. 514-525
Exhibit 62: Coin Center, <i>How Does Tornado Cash Work?</i>	A.R. 544-576
Exhibit 63: Chainalysis, <i>Crypto Mixers and AML Compliance</i>	A.R. 577-582
Exhibit 72: FIOD, <i>Arrest of Suspected Developer of Tornado Cash</i>	A.R. 629-631
Exhibit 86: GitHub, <i>Tornado Repositories/Tornado Classic UI</i>	A.R. 714-716
Exhibit 89: Crypto.com, <i>Crypto Tokens vs. Coins – What’s the Difference?</i>	A.R. 727-737
Exhibit 103: Ethereum, <i>Intro to Ethereum</i>	A.R. 814-821
Exhibit 107: Ethereum, <i>Transactions</i>	A.R. 856-872

Exhibit 108: Certik, <i>What is Blockchain Analysis?</i>	A.R. 873-883
Volume II	
Exhibit 120: Tornado Cash, <i>Introduction</i>	A.R. 950-954
Exhibit 130: National Institute of Standards and Technology, <i>Blockchain Technology Overview</i>	A.R. 1030-1152
Exhibit 157: Ethereum, <i>Decentralized Autonomous Organizations</i>	A.R. 1312-1322
Exhibit 175: ImmuneFi, <i>Tornado Cash Bug Bounties</i>	A.R. 1577-1593
Exhibit 176: Crypto News Australia, <i>Tornado Cash Token (TORN) Surges 94% Following Bullish Protocol Updates</i>	A.R. 1594-1599
Exhibit 179: Attorney General's Cyber Digital Task Force, <i>Cryptocurrency Enforcement Framework</i>	A.R. 1752-1835
Exhibit 184: BeinCrypto, <i>Ethereum Name Service (ENS): Everything You Need to Know</i>	A.R. 1931-1944
Exhibit 199: Harvard Law School Forum on Corporate Governance, <i>An Introduction to Smart Contracts and Their Potential and Inherent Limitations</i>	A.R. 2140-2149

Dated: August 18, 2023

Respectfully submitted,

Michael A. Sasso
Florida Bar No. 93814
masasso@sasso-law.com
Christian Bonta
Florida Bar No. 1010347
cbonta@sasso-law.com
SASSO & SASSO, P.A.
1031 West Morse Blvd, Suite 120
Winter Park, Florida 32789
Tel.: (407) 644-7161

/s/ Cameron T. Norris
Jeffrey M. Harris*
Cameron T. Norris*
Jeffrey S. Hetzel*
CONSOVOY MCCARTHY PLLC
1600 Wilson Boulevard, Suite 700
Arlington, VA 22209
Telephone: 703.243.9423

J. Abraham Sutherland*
106 Connally Street
Black Mountain, NC 28711
Telephone: 805.689.4577.
*pro hac vice

Counsel for Plaintiffs

CERTIFICATE OF SERVICE

I e-filed this joint appendix with the Court on August 18, 2023, which emailed everyone requiring notice. A hard copy is being mailed to the Court.

/s/ Cameron T. Norris
Counsel for Plaintiffs

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF FLORIDA
PENSACOLA DIVISION**

COIN CENTER; PATRICK O’SUL-
LIVAN; JOHN DOE; and DAVID
HOFFMAN,

Plaintiffs,

v.

JANET YELLEN, in her official ca-
pacity as Secretary of the Treasury;
DEPARTMENT OF THE TREAS-
URY; ANDREA M. GACKI, in her
official capacity as Director of the Of-
fice of Foreign Assets Control; and
OFFICE OF FOREIGN ASSETS
CONTROL,

Defendants.

Case No.

3:22-cv-20375-TKW-ZCB

JOINT APPENDIX VOLUME I



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

OFFICE OF FOREIGN ASSETS CONTROL

Case ID CYBER2-28475

DESIGNATION AND BLOCKING MEMORANDUM

The Office of Foreign Assets Control, pursuant to Executive Order 13694 of April 1, 2015, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," as amended by Executive Order 13757 of December 28, 2016, "Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities" (E.O. 13694, as amended), Executive Order 13722 of March 15, 2016, "Blocking Property of the Government of North Korea and the Workers' Party of Korea, and Prohibiting Certain Transactions with Respect to North Korea" (E.O. 13722), section 203 of the International Emergency Economic Powers Act (50 U.S.C. § 1702) (IEEPA), the National Emergencies Act (50 U.S.C. § 1601 et seq.), section 301 of title 3, United States Code, section 578.802 of the Cyber-Related Sanctions Regulations, 31 C.F.R. part 578, and section 510.802 of the North Korea Sanctions Regulations, 31 C.F.R. part 510, determines, after consultation with the Attorney General and the Secretary of State, that there is reason to believe the entity identified below and in the attached evidentiary memorandum meets one or more criteria for designation set forth in E.O. 13694, as amended, and E.O. 13722, and, therefore, is designated as a Specially Designated National or Blocked Person.

Entity

TORNADO CASH is an entity—that is, a "partnership, association, trust, joint venture, corporation, group, subgroup, or other organization"—that may be designated pursuant to IEEPA. **TORNADO CASH** is an entity with an organizational structure that consists of: (1) its founders – Alexey Pertsev, Roman Semenov, and Roman Storm – and other associated developers, who together launched the Tornado Cash mixing service, developed new Tornado Cash mixing service features, created the Tornado Cash Decentralized Autonomous Organization (DAO), and actively promote the platform's popularity in an attempt to increase its user base; and (2) the Tornado Cash DAO, which is responsible for voting on and implementing those new features created by the developers. **TORNADO CASH** is identified with the following identifiers listed below:

1. **TORNADO CASH**; Website tornado.cash; Digital Currency Address - ETH 0x12D66f87A04A9E220743712cE6d9bB1B5616B8Fc; alt. Digital Currency Address - ETH 0x47CE0C6eD5B0Ce3d3A51fdb1C52DC66a7c3c2936; alt. Digital Currency Address - ETH 0x910Cbd523D972eb0a6f4cAe4618aD62622b39DbF; alt. Digital Currency Address - ETH 0xA160cdAB225685dA1d56aa342Ad8841c3b53f291; alt. Digital Currency Address - ETH 0xD4B88Df4D29F5CedD6857912842cff3b20C8Cfa3; alt. Digital Currency Address - ETH 0xFD8610d20aA15b7B2E3Be39B396a1bC3516c7144; alt. Digital

Currency Address - ETH 0x07687e702b410Fa43f4cB4Af7FA097918ffD2730; alt.
Digital Currency Address - ETH
0x23773E65ed146A459791799d01336DB287f25334; alt. Digital Currency Address
- ETH 0x22aaA7720ddd5388A3c0A3333430953C68f1849b; alt. Digital Currency
Address - ETH 0x03893a7c7463AE47D46bc7f091665f1893656003; alt. Digital
Currency Address - ETH 0x2717c5e28cf931547B621a5dddb772Ab6A35B701; alt.
Digital Currency Address - ETH
0xD21be7248e0197Ee08E0c20D4a96DEBdaC3D20Af; alt. Digital Currency
Address - ETH 0x4736dCf1b7A3d580672CcE6E7c65cd5cc9cFBA9D; alt. Digital
Currency Address - ETH 0xDD4c48C0B24039969fC16D1cdF626eaB821d3384; alt.
Digital Currency Address - ETH
0xd96f2B1c14Db8458374d9Aca76E26c3D18364307; alt. Digital Currency Address
- ETH 0x169AD27A470D064DEDE56a2D3ff727986b15D52B; alt. Digital
Currency Address - ETH 0x0836222F2B2B24A3F36f98668Ed8F0B38D1a872f; alt.
Digital Currency Address - ETH
0x178169B423a011fff22B9e3F3abeA13414dDD0F1; alt. Digital Currency Address
- ETH 0x610B717796ad172B316836AC95a2ffad065CeaB4; alt. Digital Currency
Address - ETH 0xbB93e510BbCD0B7beb5A853875f9eC60275CF498; alt. Digital
Currency Address - ETH 0x84443CFd09A48AF6eF360C6976C5392aC5023a1F;
alt. Digital Currency Address - ETH
0xd47438C816c9E7f2E2888E060936a499Af9582b3; alt. Digital Currency Address -
ETH 0x330bdFADE01eE9bF63C209Ee33102DD334618e0a; alt. Digital Currency
Address - ETH 0x1E34A77868E19A6647b1f2F47B51ed72dEDE95DD; alt. Digital
Currency Address - ETH 0xdf231d99Ff8b6c6CBF4E9B9a945CBACeF9339178; alt.
Digital Currency Address - ETH
0xaf4c0B70B2Ea9FB7487C7CbB37aDa259579fe040; alt. Digital Currency Address
- ETH 0xa5C2254e4253490C54cef0a4347fddb8f75A4998; alt. Digital Currency
Address - ETH 0xaf8d1839c3c67cf571aa74B5c12398d4901147B3; alt. Digital
Currency Address - ETH 0x6Bf694a291DF3FeC1f7e69701E3ab6c592435Ae7; alt.
Digital Currency Address - ETH
0x3aac1cC67c2ec5Db4eA850957b967Ba153aD6279; alt. Digital Currency Address
- ETH 0x723B78e67497E85279CB204544566F4dC5d2acA0; alt. Digital Currency
Address - ETH 0x0E3A09dDA6B20aFbB34aC7cD4A6881493f3E7bf7; alt. Digital
Currency Address - ETH 0x76D85B4C0Fc497EeCc38902397aC608000A06607; alt.
Digital Currency Address - ETH
0xCC84179FFD19A1627E79F8648d09e095252Bc418; alt. Digital Currency
Address - ETH 0xD5d6f8D9e784d0e26222ad3834500801a68D027D; alt. Digital
Currency Address - ETH 0x407CcEeaA7c95d2FE2250Bf9F2c105aA7AAFB512;
alt. Digital Currency Address - ETH
0x833481186f16Cece3f1EeeA1a694c42034c3a0dB; alt. Digital Currency Address -
ETH 0xd8D7DE3349ccaA0Fde6298fe6D7b7d0d34586193; alt. Digital Currency
Address - ETH 0x8281Aa6795aDE17C8973e1aedcA380258Bc124F9; alt. Digital
Currency Address - ETH 0x57b2B8c82F065de8Ef5573f9730fC1449B403C9f; alt.
Digital Currency Address - ETH
0x05E0b5B40B7b66098C2161A5EE11C5740A3A7C45; alt. Digital Currency
Address - ETH 0x23173fE8b96A4Ad8d2E17fB83EA5dccccCa1Ae52; alt. Digital
Currency Address - ETH 0x538Ab61E8A9fc1b2f93b3dd9011d662d89bE6FE6; alt.
Digital Currency Address - ETH

0x94Be88213a387E992Dd87DE56950a9aef34b9448; alt. Digital Currency Address
- ETH 0x242654336ca2205714071898f67E254EB49ACdCe; alt. Digital Currency
Address - ETH 0x776198CCF446DFa168347089d7338879273172cF; alt. Digital
Currency Address - ETH 0xeDC5d01286f99A066559F60a585406f3878a033e; alt.
Digital Currency Address - ETH
0xD692Fd2D0b2Fbd2e52CFa5B5b9424bC981C30696; alt. Digital Currency
Address - ETH 0xca0840578f57fe71599d29375e16783424023357; alt. Digital
Currency Address - ETH 0xDF3A408c53E5078af6e8fb2A85088D46Ee09A61b; alt.
Digital Currency Address - ETH
0x743494b60097A2230018079c02fe21a7B687EAA5; alt. Digital Currency Address
- ETH 0x94C92F096437ab9958fC0A37F09348f30389Ae79; alt. Digital Currency
Address - ETH 0x5efda50f22d34F262c29268506C5Fa42cB56A1Ce; alt. Digital
Currency Address - ETH 0x2f50508a8a3d323b91336fa3ea6ae50e55f32185; alt.
Digital Currency Address - ETH
0xCee71753C9820f063b38FDbe4cFDAf1d3D928A80; alt. Digital Currency
Address - ETH 0xffbac21a641dcfe4552920138d90f3638b3c9fba; alt. Digital
Currency Address - ETH 0x179f48c78f57a3a78f0608cc9197b8972921d1d2; alt.
Digital Currency Address - ETH
0xb04E030140b30C27bcdfaafFFA98C57d80eDa7B4; alt. Digital Currency Address
- ETH 0x77777feddddfc19ff86db637967013e6c6a116c; alt. Digital Currency
Address - ETH 0x3efa30704d2b8bbac821307230376556cf8cc39e; alt. Digital
Currency Address - ETH 0x746aebc06d2ae31b71ac51429a19d54e797878e9; alt.
Digital Currency Address - ETH
0xd90e2f925DA726b50C4Ed8D0Fb90Ad053324F31b; alt. Digital Currency
Address - ETH 0x5f6c97C6AD7bdd0AE7E0Dd4ca33A4ED3fDabD4D7; alt. Digital
Currency Address - ETH 0xf4B067dD14e95Bab89Be928c07Cb22E3c94E0DAA;
alt. Digital Currency Address - ETH
0x58E8dCC13BE9780fC42E8723D8EaD4CF46943dF2; alt. Digital Currency
Address - ETH 0x01e2919679362dFBC9ee1644Ba9C6da6D6245BB1; alt. Digital
Currency Address - ETH 0x2FC93484614a34f26F7970CBB94615bA109BB4bf; alt.
Digital Currency Address - ETH
0x26903a5a198D571422b2b4EA08b56a37cbD68c89; alt. Digital Currency Address
- ETH 0xB20c66C4DE72433F3cE747b58B86830c459CA911; alt. Digital Currency
Address - ETH 0x2573BAc39EBE2901B4389CD468F2872cF7767FAF; alt. Digital
Currency Address - ETH 0x527653eA119F3E6a1F5BD18fbF4714081D7B31ce; alt.
Digital Currency Address - ETH 0x653477c392c16b0765603074f157314Cc4f40c32;
alt. Digital Currency Address - ETH
0x88fd245fEdeC4A936e700f9173454D1931B4C307; alt. Digital Currency Address
- ETH 0x09193888b3f38C82dEdfda55259A82C0E7De875E; alt. Digital Currency
Address - ETH 0x5cab7692D4E94096462119ab7bF57319726Eed2A; alt. Digital
Currency Address - ETH 0x756C4628E57F7e7f8a459EC2752968360Cf4D1AA; alt.
Digital Currency Address - ETH
0x722122dF12D4e14e13Ac3b6895a86e84145b6967; alt. Digital Currency Address -
ETH 0x94A1B5CdB22c43faab4AbEb5c74999895464Ddaf; alt. Digital Currency
Address - ETH 0xb541fc07bC7619fD4062A54d96268525cBC6FfEF; alt. Digital
Currency Address - ETH 0xD82ed8786D7c69DC7e052F7A542AB047971E73d2;
alt. Digital Currency Address - ETH
0xF67721A2D8F736E75a49FdD7FAd2e31D8676542a; alt. Digital Currency

Address - ETH 0x9AD122c22B14202B4490eDAf288FDb3C7cb3ff5E; alt. Digital
Currency Address - ETH 0xD691F27f38B395864Ea86CfC7253969B409c362d; alt.
Digital Currency Address - ETH
0xaEaaC358560e11f52454D997AAFF2c5731B6f8a6; alt. Digital Currency Address
- ETH 0x1356c899D8C9467C7f71C195612F8A395aBf2f0a; alt. Digital Currency
Address - ETH 0xA60C772958a3eD56c1F15dD055bA37AC8e523a0D; alt. Digital
Currency Address - ETH 0xBA214C1c1928a32Bffe790263E38B4Af9bFCD659; alt.
Digital Currency Address - ETH
0xb1C8094B234DcE6e03f10a5b673c1d8C69739A00; alt. Digital Currency Address
- ETH 0xF60dD140cFf0706bAE9Cd734Ac3ae76AD9eBC32A; alt. Digital Currency
Address - ETH 0x8589427373D6D84E98730D7795D8f6f8731FDA16; Secondary
sanctions risk: North Korea Sanctions Regulations, sections 510.201 and 510.210;
Transactions Prohibited For Persons Owned or Controlled By U.S. Financial
Institutions: North Korea Sanctions Regulations section 510.214; Organization
Established Date 2019 [DPRK3] [CYBER2].

Accordingly, except to the extent otherwise provided by law or unless licensed or otherwise authorized by the Office of Foreign Assets Control, (1) all real, personal, and any other property and interests in property of the entity named above that are or hereafter come within the United States, or that are or hereafter come within the possession or control of any U.S. person are blocked and may not be transferred, paid, exported, withdrawn or otherwise dealt in, and (2) any transaction or dealing by a U.S. person or within the United States in property or interests in property of the entity named above is prohibited.

Additionally, except to the extent otherwise provided by law or unless licensed or otherwise authorized by the Office of Foreign Assets Control, the following are prohibited: (1) any transaction by a United States person or within the United States that evades or avoids, has the purpose of evading or avoiding, causes a violation of, or attempts to violate, any of the prohibitions set forth in the Order; and (2) any conspiracy formed to violate any of the prohibitions set forth in E.O. 13694, as amended, and E.O. 13722.

The President has found in Section 7 of E.O. 13694, as amended, that, because of the ability to transfer funds or other assets instantaneously, prior notice to persons designated pursuant to E.O. 13694, as amended, of measures to be taken pursuant to E.O. 13694, as amended, would render these measures ineffectual. Therefore, the President determined that there need be no prior notice of such a listing or determination. In making this determination pursuant to E.O. 13694, as amended, I also find that no prior notice should be afforded to the entity named above notwithstanding the entity's prior designation because to do so would provide an opportunity to evade the measures authorized by E.O. 13694, as amended, and, consequently, render those measures ineffectual towards addressing the national emergency declared in E.O. 13694, as amended.

The President has found in Section 10 of E.O. 13722 that, because of the ability to transfer funds or other assets instantaneously, prior notice to persons designated pursuant to E.O. 13722 of measures to be taken pursuant to E.O. 13722 would render these measures ineffectual. Therefore, the President determined that there need be no prior notice of such a listing or determination. In making this determination pursuant to E.O. 13722, I also find

that no prior notice should be afforded to the entity named above notwithstanding the entity's prior designation because to do so would provide an opportunity to evade the measures authorized by E.O. 13722 and, consequently, render those measures ineffectual towards addressing the national emergency declared in E.O. 13722.

November 8, 2022

Date

Andrea M. Gacki Digitally signed by Andrea M. Gacki
Date: 2022.11.08 14:30:32 -05'00'

Andrea M. Gacki
Director
Office of Foreign Assets Control

U.S. DEPARTMENT OF THE TREASURY

Treasury Designates DPRK Weapons Representatives

November 8, 2022

Tornado Cash Redesignated with Additional DPRK Authorities, New OFAC Guidance

WASHINGTON – Today, the U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) is designating two individuals for engaging in transportation and procurement activities on behalf of the Democratic People’s Republic of Korea (DPRK). These individuals have acted on behalf of Air Koryo, an entity previously designated by OFAC for operating in the transportation industry in the DPRK economy. OFAC also delisted and simultaneously redesignated Tornado Cash under Executive Order (E.O.) 13722 and E.O. 13694, as amended. The redesignation takes into account additional information and also includes an additional basis for the designation of Tornado Cash regarding its support for DPRK activities. Tornado Cash, an entity that provides virtual currency mixing services, obfuscated the movement of over \$455 million stolen in March 2022 by the OFAC-designated, DPRK-controlled Lazarus Group in the largest known virtual currency heist to date. OFAC also issued a new Frequently Asked Question (FAQ) to provide additional compliance guidance regarding the nature of the Tornado Cash entity, and updated three existing FAQs with additional guidance.

This action is part of the United States’ ongoing efforts to limit the DPRK’s ability to advance its unlawful weapons of mass destruction (WMD) and ballistic missile programs that threaten regional stability and follows numerous recent DPRK ballistic missile launches, which are in clear violation of multiple United Nations (UN) Security Council resolutions. Continued provocation by the DPRK exemplifies the threat its unlawful weapons and missile programs pose to its neighbors, the region, international peace and security, and the global non-proliferation regime.

“Today’s sanctions action targets two key nodes of the DPRK’s weapons programs: its increasing reliance on illicit activities, including cybercrime, to generate revenue, and its ability to procure and transport goods in support of weapons of mass destruction and ballistic missile programs,” said Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E. Nelson.

INDIVIDUALS FACILITATING THE DPRK'S BALLISTIC MISSILE AND WEAPONS PROGRAMS

Air Koryo is the DPRK's national flag carrier and reportedly continues to own and operate all civilian aircraft registered in the DPRK. Air Koryo previously transported parts used in Scud-B missile systems, which fall under a UN prohibition on exporting arms and related materiel to the DPRK. According to a UN report, Air Koryo is controlled by and integrated into the DPRK military and the airline's assets are actively utilized for military purposes.

Ri Sok, an Air Koryo representative in Dandong, China, was involved in the transportation of electronic parts from China to the DPRK on behalf of the DPRK's Ministry of Rocket Industry (MORI). OFAC designated MORI on April 1, 2022 for being owned or controlled by the Munitions Industry Department (MID), an entity designated on August 30, 2010 pursuant to E.O. 13382 for its involvement with or provision of support for the DPRK's WMD and ballistic missile programs. The MID, which oversees the DPRK's ballistic missile development and nuclear weapons program, was designated by the UN on March 2, 2016.

Yan Zhiyong is a logistics manager with Air Koryo and facilitates the transportation of goods to the DPRK. Specifically, Yan Zhiyong transported goods from China to the DPRK on behalf of the Reconnaissance General Bureau (RGB), the DPRK's principal intelligence agency. The RGB, which is also involved in the DPRK's arms trade, was designated on January 2, 2015 pursuant to E.O. 13687 for being a controlled entity of the Government of the DPRK. The RGB was designated by the UN on March 2, 2016. Yan Zhiyong was the primary point of contact and intermediary for shipments destined for the DPRK and has used a Beijing-based company to transport goods into the DPRK.

Ri Sok and Yan Zhiyong are designated pursuant to E.O. 13722 for acting or purporting to act for or on behalf of, directly or indirectly, Air Koryo, a person whose property and interests in property are blocked pursuant to E.O. 13722 and who has ties to the DPRK's military activities.

REDESIGNATING TORNADO CASH

In addition to the Air Koryo representatives, OFAC simultaneously delisted and redesignated **Tornado Cash** under E.O. 13722 and E.O. 13694, as amended, for its role in enabling malicious cyber activities, which ultimately support the DPRK's WMD program. Effective immediately, the August 8, 2022 designation of Tornado Cash is no longer operative, and it is wholly replaced by today's action.

Tornado Cash is an entity that provides virtual currency mixing services through smart contracts that primarily operate on the Ethereum blockchain. The Tornado Cash smart contracts are a form of computer code that Tornado Cash uses to implement its governance structure, provide mixing services, offer financial incentives for users, increase its user base, and facilitate the financial gain of its users and developers. These smart contracts have been used by actors to obfuscate the source of funds derived from cyber heists, including funds stolen by Lazarus Group in March 2022. Malicious cyber actors subsequently used the Tornado Cash smart contracts to launder more than \$96 million of funds derived from the June 24, 2022 Harmony Bridge Heist, and at least \$7.8 million from the August 2, 2022 Nomad Heist.

Lazarus Group used the Tornado Cash smart contracts to obfuscate the source of funds derived from the March 2022 cyber heist. Lazarus Group was designated on September 13, 2019 pursuant to E.O. 13722 for being an agency, instrumentality, or controlled entity of the RGB, which has been identified as part of the Government of the DPRK. Today, OFAC is sanctioning Tornado Cash pursuant to E.O. 13722 for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, the Government of the DPRK, a person whose property and interests in property are blocked pursuant to E.O. 13722.

OFAC is also redesignating Tornado Cash pursuant to E.O. 13694, as amended, for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, a cyber-enabled activity originating from, or directed by persons located, in whole or in substantial part, outside the United States that is reasonably likely to result in, or has materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that has the purpose or effect of causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain. Specifically, the smart contracts through which Tornado Cash operates were used to obfuscate the source and destination of funds derived from Lazarus Group's March 2022 cyber heist.

SANCTIONS IMPLICATIONS

As a result of today's action, all property and interests in property of the individuals and entity designated today that are in the United States or in the possession or control of U.S. persons must be blocked and reported to OFAC. OFAC's regulations generally prohibit all dealings by

11/21/22 12:44 PM

Treasury Designates DPRK Weapons Representatives | U.S. Department of the Treasury

U.S. persons or within the United States (including transactions transiting the United States) that involve any property or interests in property of blocked or designated persons.

In addition, persons that engage in certain transactions with the individuals or entities designated today may themselves be exposed to designation. Furthermore, any foreign financial institution that knowingly facilitates a significant transaction or provides significant financial services for any of the individuals or entities designated today could be subject to U.S. correspondent or payable-through account sanctions.

The power and integrity of OFAC sanctions derive not only from its ability to designate and add persons to the Specially Designated Nationals and Blocked Persons (SDN) List but also from its willingness to remove persons from the SDN List consistent with the law. The ultimate goal of sanctions is not to punish but to bring about a positive change in behavior. For information concerning the process for seeking removal from an OFAC list, including the SDN List, please refer to OFAC's [Frequently Asked Question 897](#). For detailed information on the process to submit a request for removal from an OFAC sanctions list, please refer to [OFAC's website](#).

For additional information and guidance regarding sanctions implications specific to Tornado Cash, please reference OFAC's [FAQs 1076–1079](#) and [FAQ 1095](#).

For information on complying with virtual currency-related sanctions, please see OFAC's [Sanctions Compliance Guidance for the Virtual Currency Industry here](#) and OFAC's [FAQs on virtual currency here](#).

For more information on the individuals and entity designated today, [click here](#).

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE DECISIONAL AND DELIBERATIVE DRAFT~~



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

OFFICE OF FOREIGN ASSETS CONTROL

CYBER2-28475

EVIDENTIARY MEMORANDUM

MEMORANDUM FOR: Andrea M. Gacki
Director
Office of Foreign Assets Control

THROUGH: Ripley Quinby
Deputy Associate Director
Office of Global Targeting

[REDACTED]
Assistant Director
Russia, Europe, and Cyber Division

FROM: [REDACTED]
Acting Section Chief
Cyber and Virtual Assets Section

[REDACTED]
Sanctions Investigator
Cyber and Virtual Assets Section

[REDACTED]
Sanctions Investigator
Russia and Europe Section

SUBJECT: (U//~~FOUO~~) **TORNADO CASH**: Designation Pursuant to
Executive Order 13694 of April 1, 2015, as amended by
Executive Order 13757 of December 28, 2016; and Executive
Order 13722 of March 15, 2016

I. (U) <u>INTRODUCTION</u>	2
II. (U) <u>EXECUTIVE SUMMARY</u>	4
III. (U) <u>IDENTIFYING INFORMATION</u>	6
IV. (U) <u>BACKGROUND</u>	9
A) (U) <i>Virtual Currencies</i>	9
1) (U) Key Concepts	9
(a) (U) <i>Blockchains and Tokens</i>	9
(b) (U) <i>Smart Contracts</i>	11
(c) (U) <i>Governance</i>	12

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE DECISIONAL AND DELIBERATIVE DRAFT~~

CYBER2-29777 - 00013

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

(d) (U) <i>Illicit Finance Risks</i>	11
2) (U) Ethereum and Similar Blockchains	11
(a) (U) <i>How Ethereum Works</i>	16
(b) (U) <i>ERC-20 Tokens</i>	16
3) (U) Cryptocurrency Mixing Services	16
(a) (U) <i>Illicit Uses</i>	17
B) (U) TORNADO CASH	20
1) (U) Founders and Developers	21
2) (U) Decentralized Autonomous Organization (DAO)	25
3) (U) Smart Contracts Associated with TORNADO CASH	31
4) (U) Trusted Setup Ceremony	40
C) (U) The Tornado Cash Mixing Service	40
1) (U) How It Works	41
2) (U) How the Tornado Cash Smart Contracts Enable Mixing	41
3) (U) Anonymity Mining	44
4) (U) The Relayer Network	44
(a) (U) <i>How Relayers Work</i>	45
D) (U) TORNADO CASH's Property and Interests in Property	48
1) (U) TORNADO CASH's Interest in the Tornado Cash Smart Contracts	48
2) (U) TORNADO CASH's Interest in the TORN Smart Contract	50
3) (U) TORNADO CASH's Interest in Pool and Relayer Smart Contracts	51
E) (U) Foreign Person Property Interest Nexus	52
1) (U) Interest of North Korea	52
2) (U) Foreign Person Founders and Developers	54
3) (U) Foreign Person TORN Token Holders	54
V. (U) BASES FOR DETERMINATIONS	55
A) (U) Designation Pursuant to E.O. 13694, as Amended	55
1) (U) Sky Mavis-Ronin Bridge Heist (Cyber-Enabled Activity)	56
2) (U) TORNADO CASH	59
B) (U) Designation Pursuant to E.O. 13722	61
VI. (U) ADDITIONAL INFORMATION	64

I. (U) **INTRODUCTION**

(U) On April 1, 2015, the President issued Executive Order (E.O.) 13694, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities." [Exhibit 99]

(U) On December 28, 2016, the President issued E.O. 13757, "Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities." [Exhibit 45]

(U) E.O. 13694, as amended by E.O. 13757 ("E.O. 13694, as amended"), blocks the property and interests in property of any person determined by the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, to meet one or more of the criteria of the Order. [Exhibit 99] [Exhibit 45]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

(U) On March 15, 2016, the President issued E.O. 13722, "Blocking Property of the Government of North Korea and the Workers' Party of Korea, and Prohibiting Certain Transactions with Respect to North Korea." [Exhibit 100]

(U) E.O. 13722 blocks the property and interests in property of the GOVERNMENT OF NORTH KOREA* (the "GONK*"),¹ the WORKERS' PARTY OF KOREA* (WPK*), and of any person determined by the Secretary of the Treasury, in consultation with the Secretary of State, to meet one or more of the designation criteria of E.O. 13722. [Exhibit 100]

(U) The Office of Foreign Assets Control (OFAC) previously designated **TORNADO CASH** on August 8, 2022, pursuant to E.O. 13694, as amended;² OFAC has rescinded that designation, and OFAC has redesignated **TORNADO CASH** on the basis of the information cited herein and in the accompanying classified addendum. The redesignation takes account of additional information and includes an additional basis for the designation of **TORNADO CASH**.

~~(U//FOUO)~~ **Cyber-Enabled Activities:** Based on information presented in this memorandum and the accompanying exhibits, OFAC assesses that the *Sky Mavis-Ronin Bridge Heist*³ is a cyber-enabled activity originating from, or directed by persons located, in whole or in substantial part, outside the United States that is reasonably likely to result in, or has materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that has the purpose or effect of causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain, and thus meets the criteria for designation pursuant to section 1(a)(ii)(D) of E.O. 13694, as amended.

(U) **Material Support for Cyber-Enabled Activities:** Based on information presented in this memorandum and the accompanying exhibits, OFAC assesses that **TORNADO CASH** has materially assisted, sponsored, or provided financial, material, or technological support for, or

¹ (U) E.O. 13722 defines the GONK* to include the Government of the Democratic People's Republic of Korea (DPRK) and its agencies, instrumentalities, and controlled entities. Section 510.311 of OFAC's North Korea Sanctions Regulations, 31 C.F.R. Part 510, defines the GONK* to include, *inter alia*, (a) the state and Government of the DPRK, as well as any political subdivision, agency, or instrumentality thereof, and (b) any entity owned or controlled, directly or indirectly, by any of the foregoing, including any corporation, partnership, association, or other entity in which the GONK* owns a 50 percent or greater interest or a controlling interest, and any entity which is otherwise controlled by the GONK*.

² (U) On August 8, 2022, the U.S. Department of the Treasury designated **TORNADO CASH** pursuant to E.O. 13694, as amended, for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, a cyber-enabled activity originating from, or directed by persons located, in whole or in substantial part, outside the United States that is reasonably likely to result in, or has materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that has the purpose or effect of causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain. [Exhibit 202, p. 2]

³ (U) Throughout this memorandum, the names of targets proposed for designation will appear in **BOLD CAPITAL** letters, the name of a cyber-enabled activity described in E.O. 13694, as amended, will appear in ***Bold Italics***, and an asterisk (*) following a name in ALL CAPS denotes an individual or entity whose property and interests in property have been blocked.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

goods or services to or in support of, the *Sky Mavis-Ronin Bridge Heist*, an activity described in section 1(a)(ii) of E.O. 13694, as amended, and thus meets the criteria for designation pursuant to section 1(a)(iii)(B) of E.O. 13694, as amended.

(U//~~FOUO~~) **DPRK:** Based on information presented in this memorandum and the accompanying exhibits, OFAC assesses that **TORNADO CASH** has materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of the GONK*, a person whose property and interests in property are blocked pursuant to E.O. 13722, and thus meets the criteria for designation pursuant to section 2(a)(vii) of E.O. 13722.

(U) For these reasons, **TORNADO CASH** should be added to the List of Specially Designated Nationals and Blocked Persons (the “SDN List”) pursuant to E.O. 13694, as amended, and E.O. 13722.

II. (U) EXECUTIVE SUMMARY

(U) OFAC has designated **TORNADO CASH** for materially supporting the *Sky Mavis-Ronin Bridge Heist* and the GOVERNMENT OF NORTH KOREA* (GONK*). As part of the *Sky Mavis-Ronin Bridge Heist*, cyber actors associated with GONK* stole over \$600 million in ether (a virtual currency) from Sky Mavis, the Vietnam-based producer of a popular online game. OFAC assesses that cyber actors responsible for the *Sky Mavis-Ronin Bridge Heist* then used the Tornado Cash virtual asset mixing service, to launder the proceeds. GONK* uses funds derived from such malicious cyber activities to fund its Weapons of Mass Destruction (WMD) and ballistic missiles programs.

A. (U) **TORNADO CASH** Is an Entity that May Be Sanctioned under IEEPA

(U) As explained in *Sections IV.A – IV.B* below, **TORNADO CASH** is an entity that provides cryptocurrency mixing services through Tornado Cash and related smart contracts. Although **TORNADO CASH** purports to be only a decentralized software project, OFAC assesses that **TORNADO CASH** is an entity — that is, a “partnership, association, trust, joint venture, corporation, group, subgroup, or other organization,” that may be designated pursuant to the International Emergency Economic Powers Act, 50 U.S.C. §§ 1701-1708 (IEEPA). See section 6(b), E.O. 13694, as amended; section 9(b), E.O. 13722. **TORNADO CASH**’s organizational structure consists of: (1) its founders — Alexey Pertsev, Roman Semenov, and Roman Storm — and other associated developers, who together launched the Tornado Cash mixing service, developed new Tornado Cash mixing service features, created the Tornado Cash Decentralized Autonomous Organization (DAO), and actively promote the platform’s popularity in an attempt to increase its user base; and (2) the DAO, which is responsible for voting on and implementing new features created by the developers. In order to participate in the **TORNADO CASH** DAO, members must obtain “TORN,” a virtual token issued by **TORNADO CASH** that gives the holder the right to vote on governance measures and influence the ongoing development and maintenance of the service operated by **TORNADO CASH**. Although TORN plays an important governance function, it is also a virtual currency that may be bought and sold

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE DECISIONAL AND DELIBERATIVE DRAFT~~

on secondary markets, the value of which increases as **TORNADO CASH** increases its user base and popularity. **TORNADO CASH** uses computer code known as “smart contracts” to implement its governance structure, provide mixing services, offer financial incentives for users, increase its user base, and facilitate the financial gain of its users and developers.

(U) One of the founders has claimed that **TORNADO CASH**’s use of decentralized blockchain governance makes it “technically impossible to enforce sanctions” against **TORNADO CASH**. In fact, the evidence available to OFAC shows that **TORNADO CASH**’s governance structure in many ways mimics common corporate structures: its founders and developers operate like a board of directors, while its DAO members operate like stockholders. These features allow **TORNADO CASH** to coordinate its operations and provide a valuable service to its users, which demonstrates that it is a sanctionable entity. If decentralized blockchain governance rendered a group like **TORNADO CASH** beyond the reach of IEEPA, then any number of malicious actors could easily launder the proceeds of cyber-enabled activities like the *Sky Mavis-Ronin Bridge Heist*, merely by engaging in decentralized cryptocurrency mixing.

(U) Indeed, **TORNADO CASH** has taken concrete and coordinated steps to deploy, manage, promote, and profit from the Tornado Cash mixing service. **TORNADO CASH** has placed job advertisements. It has raised and maintained a community fund, from which it offers developers rewards for improving its code. **TORNADO CASH** has organized code deployment ceremonies, where a broader group of participants play a role in uploading changes of the service operated by **TORNADO CASH** to the Ethereum blockchain. It has refined its protocol to maximize anonymity and expand the kinds of transactions the service operated by **TORNADO CASH** can support. It has adopted qualifications and a compensation structure for “relayers,” who facilitate withdrawals from the service operated by **TORNADO CASH**. Put simply, **TORNADO CASH** is more than an open-source software protocol. Since the launch of the service operated by **TORNADO CASH**, **TORNADO CASH** has operated in a coordinated fashion, taking concrete steps to enable its users to anonymize their transactions, whether licit or illicit. These actions, taken together, demonstrate that **TORNADO CASH** is an entity, as that term is defined by E.O. 13694, as amended, and E.O. 13722.

B. (U) **TORNADO CASH** Provides a Virtual Currency Mixing Service that Allows Users to Anonymously Transmit Virtual Currency

(U) As explained in *Section IV.C* below, the service operated by **TORNADO CASH** is designed to allow users to transact in virtual currencies while maintaining their anonymity. Because blockchain transactions are recorded in publicly available blocks, it is normally possible to trace a transaction to a user’s identifiable virtual wallet. The service operated by **TORNADO CASH** attempts to address this privacy concern by allowing users to deposit virtual currencies in designated Tornado Cash virtual wallets, referred to as “anonymity pools.” Each of these anonymity pools is a “smart contract,” that is, a computer program running on the Ethereum blockchain that automatically executes a specified transaction at the request of Tornado Cash users. To use the service operated by **TORNADO CASH**, users deposit virtual assets in anonymity pools, where they are comingled with other Tornado Cash users’ assets. Users then may withdraw their assets by presenting a cryptographic note proving their ownership. By comingling the assets of Tornado Cash users within an anonymity pool, it becomes difficult for

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE DECISIONAL AND DELIBERATIVE DRAFT~~

the public to connect any particular deposit with any particular withdrawal. To enhance the privacy-protecting function of the service operated by **TORNADO CASH** even further, users may employ a third-party relayer to conduct the withdrawal on behalf of the user. The relayer charges a fee to the user and pays a separate fee to **TORNADO CASH** based on terms set by the members of the **TORNADO CASH** DAO.

C. (U) **TORNADO CASH** Has a Property Interest in the Service Operated by **TORNADO CASH** and Has a Foreign Nexus

(U) **TORNADO CASH** has a property interest in the ongoing use of the service operated by **TORNADO CASH**. As explained in *Section IV.D* below, members of the **TORNADO CASH** DAO have received TORN tokens, a valuable virtual asset that can be bought and sold on secondary markets, in connection with the development, maintenance, and management of the service operated by **TORNADO CASH**. In turn, the **TORNADO CASH** DAO has authorized the payment of TORN rewards to developers who make improvements to the service operated by **TORNADO CASH**. And, as noted above, relayers must pay **TORNADO CASH** a fee for every transaction in which a relayer acts for a user of the service operated **TORNADO CASH**. Relayers are also required to acquire and set aside a specific number of TORN tokens, which can increase the value of TORN. **TORNADO CASH** thus has an interest in the ongoing use of the service operated by **TORNADO CASH**, which generates relayer fees for **TORNADO CASH** and contributes to the overall value of TORN tokens.

(U) As explained in *Section IV.E* below, OFAC assesses that foreign persons have a substantial interest in the service operated by **TORNADO CASH**. The founders of **TORNADO CASH** reside abroad. And based on publicly available information, a substantial share of TORN token holders are foreign persons. In addition, as noted above, DPRK cyber actors have used the service operated by **TORNADO CASH** to launder the proceeds of malicious cyber activities. Because of their early and substantial use of the service operated by **TORNADO CASH**, **TORNADO CASH** has distributed TORN tokens to such DPRK users. Those DPRK users thus have an ongoing stake in the service operated by **TORNADO CASH**.

(U) The basis of OFAC's action is set forth in *Section V* below.

III. (U) **IDENTIFYING INFORMATION**

(U//~~FOUO~~) OFAC is providing the following identifiers to assist the public in identifying **TORNADO CASH** to assist in their sanctions compliance obligations, to include blocking property and interests in property of blocked persons.

1. (U) Name: **TORNADO CASH** [Exhibit 4, p. 1]
(U) Website: Tornado.Cash [Exhibit 4, p. 1]
(U) Organization Established Date: 2019 [Exhibit 120, p. 2]
(U) Ether (ETH) Digital Currency Addresses (Smart Contracts):

(U) Tornado Cash Classic Contracts:

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE DECISIONAL AND DELIBERATIVE DRAFT~~

I. 0x12D66f87A04A9E220743712cE6d9bB1B5616B8Fc
II. 0x47CE0C6eD5B0Ce3d3A51fdb1C52DC66a7c3c2936
III. 0x910Cbd523D972eb0a6f4cAe4618aD62622b39DbF
IV. 0xA160cdAB225685dA1d56aa342Ad8841c3b53f291
V. 0xD4B88Df4D29F5CedD6857912842cff3b20C8Cfa3
VI. 0xFD8610d20aA15b7B2E3Be39B396a1bC3516c7144
VII. 0x07687e702b410Fa43f4cB4Af7FA097918ffD2730
VIII. 0x23773E65ed146A459791799d01336DB287f25334
IX. 0x22aaA7720ddd5388A3c0A3333430953C68f1849b
X. 0x03893a7c7463AE47D46bc7f091665f1893656003
XI. 0x2717c5e28cf931547B621a5dddb772Ab6A35B701
XII. 0xD21be7248e0197Ee08E0c20D4a96DEBdaC3D20Af
XIII. 0x4736dCf1b7A3d580672CcE6E7c65cd5cc9cFBa9D
XIV. 0xd96f2B1c14Db8458374d9Aca76E26c3D18364307
XV. 0x169AD27A470D064DEDE56a2D3ff727986b15D52B
XVI. 0x0836222F2B2B24A3F36f98668Ed8F0B38D1a872f
XVII. 0x178169B423a011fff22B9e3F3abeA13414dDD0F1
XVIII. 0x610B717796ad172B316836AC95a2ffad065CeaB4
XIX. 0xbB93e510BbCD0B7beb5A853875f9eC60275CF498
XX. 0x84443CFd09A48AF6eF360C6976C5392aC5023a1F
XXI. 0xd47438C816c9E7f2E2888E060936a499Af9582b3
XXII. 0x330bdFADE01eE9bF63C209Ee33102DD334618e0a
XXIII. 0x1E34A77868E19A6647b1f2F47B51ed72dEDE95DD
XXIV. 0xdf231d99Ff8b6c6CBF4E9B9a945CBACeF9339178
XXV. 0xaf4c0B70B2Ea9FB7487C7CbB37aDa259579fe040
XXVI. 0xa5C2254e4253490C54cef0a4347fddb8f75A4998
XXVII. 0xaf8d1839c3c67cf571aa74B5c12398d4901147B3
XXVIII. 0x6Bf694a291DF3FeC1f7e69701E3ab6c592435Ae7
XXIX. 0x3aac1cC67c2ec5Db4eA850957b967Ba153aD6279
XXX. 0x723B78e67497E85279CB204544566F4dC5d2acA0
XXXI. 0x0E3A09dDA6B20aFbB34aC7cD4A6881493f3E7bf7
XXXII. 0x76D85B4C0Fc497EeCc38902397aC608000A06607
XXXIII. 0xCC84179FFD19A1627E79F8648d09e095252Bc418
XXXIV. 0xD5d6f8D9e784d0e26222ad3834500801a68D027D
XXXV. 0x407CcEeaA7c95d2FE2250Bf9F2c105aA7AAFB512
XXXVI. 0x833481186f16Cece3f1Eeeal a694c42034c3a0dB
XXXVII. 0xd8D7DE3349ccaA0Fde6298fe6D7b7d0d34586193
XXXVIII. 0x8281Aa6795aDE17C8973e1aedcA380258Bc124F9
XXXIX. 0x57b2B8c82F065de8Ef5573f9730fC1449B403C9f
XL. 0x05E0b5B40B7b66098C2161A5EE11C5740A3A7C45
XLI. 0x23173fe8b96A4Ad8d2E17fB83EA5dccccCa1Ae52
XLII. 0x538Ab61E8A9fc1b2f93b3dd9011d662d89bE6FE6
XLIII. 0x94Be88213a387E992Dd87DE56950a9aef34b9448
XLIV. 0x242654336ca2205714071898f67E254EB49ACdCe
XLV. 0x776198CCF446DFa168347089d7338879273172cF
XLVI. 0xeDC5d01286f99A066559F60a585406f3878a033e

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

(U) Tornado Cash Nova Contracts:

XLVII. 0xD692Fd2D0b2Fbd2e52CFa5B5b9424bC981C30696
XLVIII. 0xca0840578f57fe71599d29375e16783424023357
XLIX. 0xDF3A408c53E5078af6e8fb2A85088D46Ee09A61b
L. 0x743494b60097A2230018079c02fe21a7B687EAA5
LI. 0x94C92F096437ab9958fC0A37F09348f30389Ae79

(U) Governance Contracts:

LII. 0x5efda50f22d34F262c29268506C5Fa42cB56A1Ce
LIII. 0x2f50508a8a3d323b91336fa3ea6ae50e55f32185
LIV. 0xCEe71753C9820f063b38FDbE4cFDAf1d3D928A80
LV. 0xffbac21a641dcfe4552920138d90f3638b3c9fba
LVI. 0x179f48c78f57a3a78f0608cc9197b8972921d1d2
LVII. 0xb04E030140b30C27bcdfaafFFA98C57d80eDa7B4
LVIII. 0x7777feddddfc19ff86db637967013e6c6a116c
LIX. 0x3efa30704d2b8bbac821307230376556cf8cc39e
LX. 0x746aebc06d2ae31b71ac51429a19d54e797878e9

(U) Relayer Registry Contracts:

LXI. 0xd90e2f925DA726b50C4Ed8D0Fb90Ad053324F31b
LXII. 0x5f6c97C6AD7bdd0AE7E0Dd4ca33A4ED3fDabD4D7
LXIII. 0xf4B067dD14e95Bab89Be928c07Cb22E3c94E0DAA
LXIV. 0x58E8dCC13BE9780fC42E8723D8EaD4CF46943dF2
LXV. 0x01e2919679362dFBC9ee1644Ba9C6da6D6245BB1
LXVI. 0x2FC93484614a34f26F7970CBB94615bA109BB4bf
LXVII. 0x26903a5a198D571422b2b4EA08b56a37cbD68c89
LXVIII. 0xB20c66C4DE72433F3cE747b58B86830c459CA911
LXIX. 0x2573BAc39EBE2901B4389CD468F2872cF7767FAF

(U) Other Contracts:

LXX. 0x527653eA119F3E6a1F5BD18fbF4714081D7B31ce
LXXI. 0x653477c392c16b0765603074f157314Cc4f40c32
LXXII. 0x88fd245fEdeC4A936e700f9173454D1931B4C307
LXXIII. 0x09193888b3f38C82dEdfda55259A82C0E7De875E
LXXIV. 0x5cab7692D4E94096462119ab7bF57319726Eed2A
LXXV. 0x756C4628E57F7e7f8a459EC2752968360Cf4D1AA
LXXVI. 0x722122dF12D4e14e13Ac3b6895a86e84145b6967
LXXVII. 0x94A1B5CdB22c43faab4AbEb5c74999895464Ddaf
LXXVIII. 0xb541fc07bC7619fD4062A54d96268525cBC6FfEF
LXXIX. 0xD82ed8786D7c69DC7e052F7A542AB047971E73d2
LXXX. 0xDD4c48C0B24039969fC16D1cdF626eaB821d3384 [Exhibit 177, pp. 1–9]
LXXXI. 0xF67721A2D8F736E75a49FdD7FAd2e31D8676542a
LXXXII. 0x9AD122c22B14202B4490eDAf288FDb3C7cb3ff5E
LXXXIII. 0xD691F27f38B395864Ea86CfC7253969B409c362d
LXXXIV. 0xaEaaC358560e11f52454D997AAFF2c5731B6f8a6

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

LXXXV. 0x1356c899D8C9467C7f71C195612F8A395aBf2f0a
LXXXVI. 0xA60C772958a3eD56c1F15dD055bA37AC8e523a0D
LXXXVII. 0xBA214C1c1928a32Bffe790263E38B4Af9bFCD659
LXXXVIII. 0xb1C8094B234DcE6e03f10a5b673c1d8C69739A00
LXXXIX. 0xF60dD140cFf0706bAE9Cd734Ac3ae76AD9eBC32A

[Exhibit 101, pp. 2–10]

(U) Ether (ETH) Digital Currency Addresses (Externally Owned Account):

I. 0x8589427373D6D84E98730D7795D8f6f8731FDA16

[Exhibit 195, p. 1]

IV. BACKGROUND

(U) This section summarizes and explains information necessary to understand **TORNADO CASH** and its operations.

- (U) Part A details key information related to virtual currencies, including key concepts, how Ethereum and similar blockchains function, and how cryptocurrency mixing services relate to the broader cryptocurrency ecosystem.
- (U) Part B details **TORNADO CASH** and key aspects of how this entity operates.
- (U) Part C details the Tornado Cash mixing service. Throughout this memorandum, OFAC will refer to the entity proposed for designation with the bold and capitalized “**TORNADO CASH**.” OFAC will use “Tornado Cash” without bolding or capitalization when that term serves as a descriptor, such as in “the Tornado Cash smart contracts.” When directly quoting from sources, OFAC retains the formatting used in the source. Some of the sources also refer to Tornado.Cash, which refers to the domain which hosted some of the resources associated with the entity and its services.
- (U) Part D describes **TORNADO CASH**’s property and interests in property.
- (U) Part E details the property interest of foreign persons in **TORNADO CASH**.

A. (U) *Virtual Currencies*

1. (U) *Virtual Currencies: Key Concepts*

a. (U) *Virtual Currencies: Blockchains and Tokens*

(U) According to an October 2020 U.S. Department of Justice Report of the Attorney General’s Cyber-Digital Task Force (the “Cyber-Digital Task Force Report”), “virtual currency” is a digital representation of value that, like traditional coin and paper currency, functions as a medium of exchange—i.e., it can be digitally traded or transferred, and can be used for payment or investment purposes. Virtual currency is a type of “virtual asset” that is separate and distinct from digital representations of traditional currencies, securities, and other traditional financial assets. “Cryptocurrency” refers to a specific type of virtual currency with key characteristics. The vast majority of cryptocurrencies are decentralized, in that they lack a central administrator

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

to issue currency and maintain payment ledgers⁴—in other words, there is no central bank. Instead, cryptocurrencies rely on complex algorithms, a distributed ledger that is often referred to as the “blockchain,” and a network of peer-to-peer⁵ users to maintain an accurate system of payments and receipts. Some examples of cryptocurrencies include Bitcoin, Litecoin, and Ether. [Exhibit 179, pp. 14–15]

(U) According to the website of Crypto.com, “like crypto coins, crypto tokens are designed using blockchain technology; however, crypto tokens aren’t native to a blockchain. Instead, they’re built on top of it, often utilizing smart contracts⁶ to fulfil a variety of purposes. While crypto coins mimic traditional currencies, crypto tokens are more like assets or even deeds. A crypto token can represent a share of ownership in a Decentralized Autonomous Organization (DAO),⁷ a digital product or non-fungible token (NFT),⁸ or even a physical object. Crypto tokens can be bought, sold, and traded like coins, but they aren’t used as a medium of exchange. To use a real-world example, crypto tokens are more like coupons or vouchers, while crypto coins are like dollars and cents. There are numerous types of crypto tokens: Some governance tokens offer holders voting rights in a DAO. Certain tokens, known as “utility tokens” may provide access to certain services or products developed by the token issuer. Most crypto tokens are designed to be used within a blockchain project or decentralized app (or “dapp”).⁹ Unlike crypto coins, tokens are created and distributed by the project developer for the particular intended purpose or use of those tokens. Once tokens are in the hands of purchasers, they can be used in accordance with their design. For example, Axie Infinity, one of the best-known play-to-earn (P2E) [games] on the market, features a utility token called Smooth Love Potions (SLP). By earning or purchasing SLP, players can perform exclusive in-game tasks.” [Exhibit 89, p. 4]

(U) According to the Cyber-Digital Task Force Report, cryptocurrency can be exchanged directly person to person; through a cryptocurrency exchange; or through other intermediaries. The storage of cryptocurrency is typically associated with an individual “wallet,” which is similar to a virtual account. Wallets can interface with blockchains and generate and/or store the public keys (which are roughly akin to a bank account number) and private keys (which function like a PIN or password) that are used to send and receive cryptocurrency. [Exhibit 179, p. 15]

⁴ (U) According to an October 2018 NIST report, a ledger is a record of transactions. [Exhibit 130, p. 63]

⁵ (U) According to a May 17, 2022, Cointelegraph article, accessed on October 1, 2022, peer-to-peer (P2P) trading is a type of cryptocurrency exchange method that allows traders to trade directly with one another without the need for a centralized third party to facilitate the transactions. [Exhibit 152, p. 2] According to Cointelegraph’s website, Cointelegraph was founded in 2013 and is the leading independent digital media resource covering a wide range of news on blockchain technology, crypto assets, and emerging fintech trends. [Exhibit 23, p. 1]

⁶ (U) Smart contracts are further explained in *Section IV.A.2 (Virtual Currencies: Ethereum)* below.

⁷ (U) According to the “Decentralized Autonomous Organizations” page of Ethereum’s website, [REDACTED] a DAO is a Decentralized Autonomous Organization which is member-owned community without centralized leadership. [Exhibit 157, p. 1] DAOs will be explained in detail in *Section IV.B.2 (TORNADO CASH: Decentralized Autonomous Organization (DAO))* below.

⁸ (U) According to a Cointelegraph article, nonfungible tokens, or NFTs, are verifiably unique representations of digital and physical goods. Each NFT generally differs in makeup, and therefore likely differs in value as well. [Exhibit 115, p. 1]

⁹ (U) Decentralized Apps are further described in *Section IV.A.2 (Virtual Currencies: Ethereum)* section below.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

(U) According to a September 24, 2021, Council on Foreign Relations¹⁰ report, cryptocurrency users send funds between digital wallet addresses. These transactions are then recorded into “blocks,” and confirmed across the network. Blockchains do not record real names or physical addresses, only the transfers between digital wallets, and thus confer a degree of anonymity on users. However, if the identity of a wallet owner becomes known, their transactions can be traced. The prices of Bitcoin and many other cryptocurrencies vary based on global supply and demand. [Exhibit 110, pp. 1–2]

b. (U) Virtual Currencies: Smart Contracts

(U//~~FOUO~~) As described in Section IV.B.2 (**TORNADO CASH: Decentralized Autonomous Organization (DAO)**), TORNADO CASH uses smart contracts to implement its governance structure. As described below in Section IV.C.2 (**The Tornado Cash Mixing Service: How the Tornado Cash Smart Contracts Enable Mixing**), TORNADO CASH deployed smart contracts to multiple blockchains to operationalize its mixing service.

(U) According to the website of Ethereum, “Ethereum calls the programs uploaded to and executed by the network smart contracts. At a very basic level, you can think of a smart contract like a sort of vending machine: a script that, when called with certain parameters, performs some actions or computation if certain conditions are satisfied. For example, a simple vendor smart contract could create and assign ownership of a digital asset¹¹ if the caller sends ETH to a specific recipient. Because developers can write arbitrary executable applications into the Ethereum Virtual Machine¹² (EVM) by publishing smart contracts, these are often also called DApps, or Decentralized Apps.” [Exhibit 103, pp. 4–6]

(U) According to a May 26, 2018 post on the website of the Harvard Law School Forum on Corporate Governance, “smart contracts” is a term used to describe computer code that automatically executes all or parts of an agreement and is stored on a blockchain-based platform. Before a compiled smart contract actually can be executed on certain blockchains, an additional step is required, namely, the payment of a transaction fee for the contract to be added to the chain and executed upon. In the case of the Ethereum blockchain, smart contracts are executed on the EVM, and this payment, made through the ether cryptocurrency, is known as “gas.” The more complex the smart contract (based on the transaction steps to be performed), the more gas that must be paid to execute the smart contract. Thus, gas currently acts as an important gate to

¹⁰ (U) According to its website, the Council on Foreign Relations is an independent, nonpartisan membership organization, think tank, and publisher dedicated to being a resource for its members, government officials, business executives, journalists, educators and students, civic and religious leaders, and other interested citizens in order to help them better understand the world and the foreign policy choices facing the United States and other countries. Founded in 1921, CFR takes no institutional positions on matters of policy. [Exhibit 82, p. 7]

¹¹ (U) According to an October 2018 NIST report, a digital asset is any asset that is purely digital, or is a digital representation of a physical asset. [Exhibit 130, p. 62]

¹² (U) According to the website of Ethereum, [REDACTED] the Ethereum Virtual Machine is the global virtual computer whose state every participant can request the execution of arbitrary code on the EVM; code execution changes the state of the EVM. [Exhibit 103, p. 5]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

prevent overly complex or numerous smart contracts from overwhelming the EVM. [Exhibit 199, p. 1]

c. (U) Virtual Currencies: Governance

(U) According to an October 2018 National Institute of Science and Technology (NIST) report, the “governance” of blockchain networks refers to the rules, practices, and processes by which the blockchain network is directed and controlled. A common misconception is that blockchain networks are systems without control and ownership. This is not strictly true. Permissioned blockchain networks are generally set up and run by an owner or consortium, which governs the blockchain network. Permissionless blockchain networks are often governed by blockchain network users, publishing nodes,¹³ and software developers. [Exhibit 130, p. 46]

(U) According to a June 27, 2022 blog post by Chainalysis,¹⁴ Decentralized Autonomous Organizations (DAOs) are intended to provide a new, democratized management structure for businesses, projects, and communities, in which any member can vote on organizational decisions just by buying into the project. At a high level, this is how DAOs work:

1. DAO founders create a new cryptocurrency, known as a governance token;
2. They distribute these tokens to users, backers, and other stakeholders; and
3. Each token corresponds to a set amount of voting power within the organization. It also corresponds to a price on the secondary market, where it can be bought and sold at will.

[Exhibit 59, p. 1]

(U) According to Chainalysis, while this process is often described as a way to decentralize power, governance token data suggests that DAO ownership is highly concentrated. By analyzing the distribution of ten major DAOs’ governance tokens, Chainalysis finds that, across several major DAOs, less than 1 percent of all holders have 90 percent of the voting power. This has meaningful implications for DAO governance. For example, if just a small portion of the top 1% of holders worked together, they could theoretically outvote the remaining 99% on any decision. This has obvious practical implications and, in terms of investor sentiment, likely affects whether small holders feel that they can meaningfully contribute to the proposal process. [Exhibit 59, pp. 1–2]

d. (U) Virtual Currencies: DPRK Illicit Finance Risks

(U) According to the U.S. Department of the Treasury’s 2022 National Proliferation Financing Risk Assessment (NPFRA), the DPRK’s malicious cyber activities are an important source of

¹³ (U) According to NIST, a node is an individual system within a blockchain network: 1. Full Node — a node that stores the entire blockchain, ensures transactions are valid, a publishing node is a node that, in addition to all responsibilities required of a full node, is tasked with extending the blockchain by creating and publishing new blocks. Also known as mining node, committing node, minting node. 2. Lightweight Node — a node that does not store or maintain a copy of the blockchain and must pass their transactions to full nodes. [Exhibit 130, p. 14]

¹⁴ (U) According to the “About Us” page of its website, [REDACTED] Chainalysis provides blockchain-related data, software, services, and research to government agencies, exchanges, financial institutions, and insurance and cybersecurity companies in over 60 countries. Their data powers investigations, compliance, and market intelligence software that has been used to solve some of the world’s most high-profile criminal cases and grow consumer access to virtual currency safely. [Exhibit 26, p. 1]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

revenue generation for its military budget. In April 2020, the Departments of State, the Treasury, Homeland Security, and Justice co-published a DPRK Cyber Threat Advisory that highlighted the DPRK's malicious cyber activities and how the DPRK has targeted financial institutions and other private sector actors to fulfill its foreign policy ends. These include (1) disrupting critical infrastructure; (2) targeting those critical of the regime; (3) engaging in cyber-enabled financial theft and money laundering; and (4) compromising computers and network systems to generate virtual assets (a technique known as "cryptojacking"). DPRK state-sponsored cyber actors are subordinate to the RECONNAISSANCE GENERAL BUREAU* (RGB*),¹⁵ the DPRK's main intelligence agency and a UN- and U.S.-designated entity. [Exhibit 200, p. 9]

(U) According to the NPFRA, proliferation financing¹⁶ networks are increasingly exploiting the digital economy, including by engaging in the systematic mining and trading of virtual assets and the hacking of virtual asset service providers (VASPs). The DPRK's capacity and willingness to engage in increasingly sophisticated malicious cyber activity, against both traditional financial institutions, such as central banks and private firms, and the virtual assets sector, have grown considerably since 2018. There is no evidence that a proliferation network has used a virtual asset to procure a specific proliferation-sensitive good or technology¹⁷ as an input to a WMD or ballistic missile program. However, virtual assets play an essential role in revenue generation and moving assets across borders. States and groups that are involved in exploiting the digital economy for sanctions evasion have used existing virtual assets, like Bitcoin, Ether, XRP, and Litecoin, among others. Hackers affiliated with or linked to the DPRK have conducted a broad range of criminal cyber activity to "further the strategic and financial interests of the DPRK government and its leader, Kim Jong-un." In many cases, the activities directly target U.S. individuals and companies (including, but not limited to, financial institutions). In April 2020, the Departments of State, Homeland Security, and the Treasury, along with the FBI, released Guidance on the North Korean Cyber Threat to provide a comprehensive resource on how cyber actors linked to the DPRK threaten both "traditional" financial institutions as well as new financial technology companies, especially VASPs. Proliferation networks are increasingly embracing certain types of virtual assets that enhance user anonymity. This activity is a significant source of revenue raised in violation of U.S. and UN sanctions. [Exhibit 200, pp. 1, 29–30]

(U) As explained in detail in Exhibits 54, 65, and 114, to address the illicit finance risks posed by virtual currencies, the U.S. Department of the Treasury has designated multiple persons under its sanctions authorities:

¹⁵ (U) On January 2, 2015, OFAC blocked the property and interests in property of the RECONNAISSANCE GENERAL BUREAU* (RGB*) pursuant to E.O. 13687, "Imposing Additional Sanctions With Respect To North Korea". [Exhibit 149, pp. 2–3] The RGB* was listed in the annex to E.O. 13551 of August 30, 2010, "Blocking Property of Certain Persons With Respect to North Korea." [Exhibit 2, p. 4]

¹⁶ (U) According to the NPFRA, financing of proliferation refers to the risk of raising, moving, or making available funds, other assets or economic resources, or financing, in whole or in part, to persons or entities for purposes of WMD proliferation, including the proliferation of their means of delivery or related material (including both dual-use technologies and dual-use goods for non-legitimate purposes). [Exhibit 200, p. 4]

¹⁷ (U) Given the context of this exhibit, OFAC assesses that "proliferation sensitive good or technology" references goods or technology that can be used in the development of WMD, including dual-use technologies or related material.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE DECISIONAL AND DELIBERATIVE DRAFT~~

- On September 21, 2021, the U.S. Department of the Treasury designated the virtual currency exchange Suex;
- On May 6, 2022, the U.S. Department of the Treasury designated the virtual currency mixer Blender.io;
- On November 8, 2021 the U.S. Department of the Treasury designated the virtual currency exchange Chatex; and
- On April 5, 2022 the U.S. Department of the Treasury designated the virtual currency exchange Garantex and the Darknet Market Hydra Market.

(U//~~FOUO~~) Summarizing the above, this section explained following core concepts necessary to understand **TORNADO CASH**:

- (U//~~FOUO~~) Blockchains are a form of distributed database that may record ownership of virtual assets that are known as virtual currencies or cryptocurrencies.
- (U//~~FOUO~~) Smart contracts are applications built on blockchain networks that execute specified tasks.
- (U//~~FOUO~~) Blockchains and smart contracts can be employed to enable new forms of governance and governance structures, such as Decentralized Autonomous Organizations.
- (U//~~FOUO~~) Decentralized Autonomous Organizations are blockchain-enabled management structures in which individuals who obtain tokens can vote on organizational decisions.
- (U//~~FOUO~~) Virtual currencies and blockchains have created new illicit finance vulnerabilities that have been exploited by threat actors.

2. (U) *Virtual Currencies: Ethereum*

(U//~~FOUO~~) As detailed in *Section IV.B (TORNADO CASH)*, and *Section IV.C (The Tornado Cash Mixing Service)*, Tornado Cash smart contracts have been deployed primarily on the Ethereum blockchain. This subsection provides additional background and defines terminology specific to Ethereum.

a. (U) *Ethereum: How Ethereum Works*

(U) According to the website of Ethereum, “transactions are cryptographically signed instructions from accounts. An account will initiate a transaction to update the state of the Ethereum network. The simplest transaction is transferring ETH from one account to another. An Ethereum transaction refers to an action initiated by an externally owned account, in other words an account managed by a human, not a contract. For example, if Bob sends Alice 1 ETH, Bob’s account must be debited and Alice’s must be credited. This state-changing action takes place within a transaction. Transactions, which change the state of the Ethereum Virtual Machine (EVM), need to be broadcast to the whole network. Any node can broadcast a request for a transaction to be executed on the EVM; after this happens, a validator¹⁸ will execute the

¹⁸ (U) According to the website of Ethereum, [REDACTED] it takes a 32 ETH [deposit] to activate validator software. As a validator you will be responsible for storing data, processing transactions, and adding new

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

transaction and propagate the resulting state change to the rest of the network. Transactions require a fee and must be included in a validated block Transaction Lifecycle. Once the transaction has been submitted the following happens:

- Once you send a transaction, cryptography generates a transaction hash.
- The transaction is then broadcast to the network and included in a pool with lots of other transactions.
- A validator must pick your transaction and include it in a block in order to verify the transaction and consider it “successful.”
- As time passes, the block containing your transaction will be upgraded to “justified” then “finalized.” These upgrades make it much more certain that your transaction was successful and will never be altered. Once a block is “finalized,” it could only ever be changed by an attack that would cost many billions of dollars.”

[Exhibit 107, pp. 1–2, 13]

(U) According to the website of Ethereum, Ether (ETH) is the native cryptocurrency of the Ethereum blockchain. Any participant who broadcasts a transaction request must also offer some amount of ETH to the network as a “bounty.” The network will award this bounty to whoever eventually does the work of verifying the transaction, executing it, committing it to the blockchain, and broadcasting it to the network. The amount of ETH paid corresponds to the time required to do the computation. [Exhibit 103, p. 4]

(U) According to the website of Ethereum, an Ethereum account is an entity with an ETH balance that can send transactions on the Ethereum blockchain. Accounts can be user-controlled or deployed as smart contracts. There are two Ethereum account types: *externally owned*, or controlled by anyone with the corresponding private keys,¹⁹ and a *smart contract*²⁰ deployed to the Ethereum protocol network and controlled by code. The key differences are:

- Externally owned:
 - Creating an account costs nothing;
 - Can initiate transactions;
 - Transactions between externally owned accounts can only be ETH/token transfers.
- Smart contract:
 - Creating a contract has a cost because you are using network storage;
 - Can only send transactions in response to receiving a transaction;
 - Transactions from an external account to a contract account can trigger code that can execute many different actions, such as transferring tokens or even creating a new contract. [Exhibit 58, pp. 1–2]

blocks to the blockchain. This will keep Ethereum secure for everyone and earn you new ETH in the process. [Exhibit 221, p. 21] OFAC assesses that anyone with 32 ETH can opt in to become a validator by taking 32 ETH

¹⁹ (U//FOUO) [REDACTED]

[Exhibit 27, p. 44]

²⁰ (U//FOUO) The exhibit refers to “contract” rather than “smart contract.” Because these terms are used interchangeably in this exhibit, OFAC assesses that all Ethereum contracts referenced in this exhibit are smart contracts.

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~
PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT

(U//FOUO)

[Exhibit 106, p. 6]

b. (U) Ethereum: ERC-20 Tokens

(U//FOUO) As will be described in *Section IV.B (TORNADO CASH)* and *Section IV.C (The Tornado Cash Mixing Service)*, TORNADO CASH uses a token called TORN to manage its governance and distribute income derived from TORNADO CASH's operations. TORNADO CASH created TORN (an ERC-20 token) as a smart contract deployed on the Ethereum blockchain contract.

(U) According to Investopedia, "ERC-20" refers to a scripting standard used within the Ethereum blockchain. This technical standard dictates a number of rules and actions that an Ethereum token or smart contract must follow and steps to be able to implement it. It is perhaps easiest to think of ERC-20 as a set of basic guidelines and functions that any new token created in the Ethereum network must follow. [Exhibit 21, p. 4]

3. (U) Virtual Currencies: Mixing Services

(U//FOUO) As will be described in *Section IV.B (TORNADO CASH)* and *Section IV.C (The Tornado Cash Mixing Service)*, the purpose of TORNADO CASH and the Tornado Cash smart contracts is to provide a non-custodial²¹ cryptocurrency mixing service.

(U) According to the Cyber-Digital Task Force Report, "mixers" and "tumblers"²² are entities that attempt to obfuscate the source or owner of particular units of cryptocurrency by mixing the cryptocurrency of several users prior to delivery of the units to their ultimate destination. For a fee, a customer can send cryptocurrency to a specific address that is controlled by the mixer. The mixer then commingles this cryptocurrency with funds received from other customers before sending it to the requested recipient address. [Exhibit 179, p. 53]

(U) According to a February 18, 2022 blogpost on CERTIK's²³ website, one of the primary purposes of blockchain analysis is to trace the flow of funds between addresses. This may be to follow the proceeds of an exploit,²⁴ or to establish a transaction chain linking two or more

²¹ (U) According to the website of Gemini, [REDACTED] with a non-custodial wallet, you have sole control of your private keys, which in turn control your cryptocurrency and prove the funds are yours. With a custodial wallet, another party controls your private keys. Most custodial wallets these days are web-based exchange wallets. [Exhibit 226, p. 1] According to its website, Gemini is a crypto exchange that is a New York trust company regulated by the New York State Department of Financial Services. [Exhibit 227, p. 2]

²² (U//FOUO) OFAC uses the terms "mixer" and "tumbler" interchangeably in this memorandum.

²³ (U) According to its website, CERTIK is a pioneer in blockchain security, utilizing best-in-class Formal Verification and AI technology to secure and monitor blockchains, smart contracts, and Web3 apps. [Exhibit 109, p. 1]

²⁴ (U//FOUO)

[Exhibit 53, p. 15]

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~
PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

wallets. The immutability of blockchains makes the technology well-suited to establishing historical claims and chains of strong correlation. [Exhibit 108, p. 3]

(U) According to an August 23, 2022 blog post by Chainalysis, a cryptocurrency mixer is a service that blends the cryptocurrencies of many users together to obfuscate the origins and owners of the funds. Because Bitcoin, Ethereum, and most other public blockchains are transparent, this level of privacy is otherwise hard to achieve. Mixers collect, pool, and pseudo-randomly²⁵ shuffle the cryptocurrencies deposited by many users. Later, the funds are withdrawn to new addresses under the control of each user. [Exhibit 63, pp. 1–2]

(U) According to an August 23, 2022 blog post by Chainalysis, centralized custodial mixers, which emerged as early as 2011, temporarily take ownership of users' funds and are typically run by a single operator. Because this type of mixing service is both centralized and custodial, users face additional privacy risks. They are also often a target of law enforcement, as financial enforcement agencies treat them as unregistered money services businesses. [Exhibit 63, p. 3]

(U) According to an August 23, 2022 blog post by Chainalysis, smart contract mixers²⁶ are non-custodial and do not combine users' funds in just one transaction. Instead, the user sends their funds to the mixer, receives a cryptographic note proving that they are the depositor, and then, whenever they would like, sends the mixer that note to withdraw the funds to a new address. [Exhibit 63, p. 3]

a. (U) *Mixing Services: Illicit Uses*

(U) According to a July 14, 2022 blog post by Chainalysis, “crypto[currency] mixers are a go-to tool for cybercriminals on the blockchain. Chainalysis finds that in 2022, crypto addresses tied to illicit activity transferred nearly 10 percent of their funds to mixers — with no other address type sending more than 0.3 percent. Cryptocurrency mixers saw significant quarter-over-quarter volume increases starting in 2020 and continuing through 2021. While that growth has leveled off somewhat this year, it remains close to all-time highs. The increases come primarily from growth in the volume sent from centralized exchanges, DeFi²⁷ protocols, and most notably, addresses connected to illicit activity. Illicit addresses account for 23 percent of funds sent to mixers so far in 2022, up from 12 percent in 2021. What stands out most is the huge volume of funds moving to mixers from addresses associated with sanctioned entities, especially in Q2 2022. [Exhibit 116, pp. 1, 3–5]

(U) According to a February 2022 Chainalysis report, North Korean cybercriminals had a banner year in 2021, launching at least seven attacks on cryptocurrency platforms that extracted nearly

²⁵ (U) According to PCMag, pseudo-random numbers provide necessary values for processes that require randomness. It is called “pseudo” random, because the algorithm can repeat the sequence, and the numbers are thus not entirely random. [Exhibit 228, p. 1]

²⁶ (U//FOUO) As explained in Sections IV.B (*TORNADO CASH*) and IV.C (*The Tornado Cash Mixing Service*), *TORNADO CASH* provides smart contract mixing services.

²⁷ (U) According to Investopedia, Decentralized Finance (DeFi) is an emerging financial technology based on secure distributed ledgers similar to those used by cryptocurrencies. DeFi eliminates the fees that banks and other financial companies charge for using their services. Individuals hold money in a secure digital wallet, can transfer funds in minutes, and anyone with an internet connection can use DeFi. [Exhibit 203, p. 1]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE DECISIONAL AND DELIBERATIVE DRAFT~~

\$400 million worth of digital assets last year. These attacks targeted primarily investment firms and centralized exchanges, and made use of phishing²⁸ lures, code exploits, malware,²⁹ and advanced social engineering³⁰ to siphon funds out of these organizations' internet-connected "hot" wallets³¹ into DPRK-controlled addresses. Once North Korea gained custody of the funds, they began a careful laundering process to cover up and cash out. This is especially true for APT 38, also known as "LAZARUS GROUP*,"³² which is led by DPRK's primary intelligence agency, the U.S.- and UN-sanctioned RECONNAISSANCE GENERAL BUREAU*.³³ While Chainalysis will refer to the attackers as North Korean-linked hackers more generally, many of these attacks were carried out by the LAZARUS GROUP* in particular. LAZARUS GROUP* first gained notoriety from its Sony Pictures and WannaCry cyberattacks, but it has since concentrated its efforts on cryptocurrency crime — a strategy that has proven immensely profitable. From 2018 on, the group has stolen and laundered massive sums of virtual currencies every year, typically in excess of \$200 million. The most successful individual hacks, one on KuCoin and another on an unnamed cryptocurrency exchange, each netted more than \$250 million alone. And according to the UN Security Council, the revenue generated from these hacks goes to support North Korea's WMD and ballistic missile programs. [Exhibit 178, p. 114]

(U) According to the same Chainalysis report, in 2021, North Korean hacking activity was on the rise once again. From 2020 to 2021, the number of North Korean-linked hacks jumped from four to seven, and the value extracted from these hacks grew by 40 percent. Interestingly, in terms of dollar value, Bitcoin now accounts for less than one fourth of the cryptocurrencies stolen by DPRK. In 2021, only 20% of the stolen funds were Bitcoin, whereas 22 percent were either ERC-20 tokens or altcoins.³⁴ For the first time ever, ETH accounted for a majority of the

²⁸ (U//FOUO) [REDACTED]

[Exhibit 53, p. 25]

²⁹ (U//FOUO) [REDACTED]

[Exhibit 53, p. 21]

³⁰ (U//FOUO) [REDACTED]

[Exhibit 53, p. 28]

³¹ (U) According to Investopedia, [REDACTED] a hot wallet is a cryptocurrency wallet that is always connected to the internet and cryptocurrency network. Hot wallets are used to send and receive cryptocurrency, and they allow you to view how many tokens you have available to use. [Exhibit 47, p. 3]

³² (U) On September 13, 2019, the Department of the Treasury identified the LAZARUS GROUP* as meeting the definition of the Government of North Korea as set forth in section 9(d) of Executive Order 13722 because it is an agency, instrumentality, or controlled entity of the Government of North Korea. [Exhibit 113, p. 1]

³³ (U) On January 2, 2015, OFAC blocked the property and interests in property of the RECONNAISSANCE GENERAL BUREAU* (RGB*) pursuant to E.O. 13687, "Imposing Additional Sanctions With Respect To North Korea". [Exhibit 149, pp. 2–3] RGB* was listed in the annex to E.O. 13551 of August 30, 2010. [Exhibit 2, p. 4]

³⁴ (U) According to Investopedia, altcoins are generally defined as all cryptocurrencies other than Bitcoin. However, some people consider altcoins to be all cryptocurrencies other than Bitcoin and Ethereum because most cryptocurrencies are forked from one of the two. [Exhibit 187, p. 4] According to the website of makeuseof.com, [REDACTED] the term "forking" has been used within the software development community for decades. At the inception of its usage, "forking" mainly referred to copying a piece of software and then developing it parallel to its trunk copy. But the term's meaning evolved over time and now defines a specific phenomenon in software development. Software is "forked" when a rift occurs within its developing team, which could be due to

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

funds stolen at 58 percent. The growing variety of cryptocurrencies stolen has necessarily increased the complexity of DPRK's cryptocurrency laundering operation. Today, DPRK's typical laundering process is as follows:

1. ERC-20 tokens and altcoins are swapped for ETH via decentralized exchange (DEX)
2. ETH is mixed
3. Mixed ETH is swapped for Bitcoin via DEX
4. Bitcoin is mixed
5. Mixed Bitcoin is consolidated into new wallets
6. Bitcoin is sent to deposit addresses at crypto-to-fiat exchanges based in Asia—potential cash-out points. [Exhibit 178, pp. 115–117]

(U) According to the same Chainalysis report, Chainalysis observed a massive increase in the use of mixers among DPRK-linked actors in 2021. More than 65 percent of DPRK's stolen funds were laundered through mixers this year, up from 42 percent in 2020 and 21 percent in 2019, suggesting that these threat actors have taken a more cautious approach with each passing year. The DPRK is a systematic money launderer, and their use of multiple mixers — software tools that pool and scramble cryptocurrencies from thousands of addresses — is a calculated attempt to obscure the origins of their ill-gotten cryptocurrencies while off ramping³⁵ into fiat. DeFi platforms like DEXs provide liquidity for a wide range of ERC-20 tokens and altcoins that may not otherwise be convertible into cash. When DPRK swaps these coins for ETH or BTC they become much more liquid, and a larger variety of mixers and exchanges become usable. Moreover, DeFi platforms do not take custody of user funds and many do not collect know-your-customer (KYC) information, meaning that cybercriminals can use these platforms without having their assets frozen or their identities exposed. [Exhibit 178, pp. 115–117]

(U) According to OFAC's Frequently Asked Question #561, published on OFAC's website on March 19, 2018, the United States' whole-of-government strategies to combat global threats such as terrorism, transnational organized crime, malicious cyber activity, narcotics trafficking, WMD proliferation, and human rights abuses include targeting an array of activities, including the use of digital currencies or other emerging payment systems to conduct proscribed financial transactions and evade U.S. sanctions. The strategies draw from a broad range of tools and authorities to respond to the growing and evolving threat posed by malicious actors using new payment mechanisms. OFAC will use sanctions in the fight against criminal and other malicious actors abusing digital currencies and emerging payment systems as a complement to existing tools, including diplomatic outreach and law enforcement authorities. To strengthen our efforts to combat the illicit use of digital currency transactions under our existing authorities, OFAC may include as identifiers on the SDN List specific digital currency addresses associated with blocked persons. [Exhibit 117, p. 2]

differences of opinion regarding the project's direction or personality clashes. A faction or member of the development team will then take the program's source code and start independent development under a different name, approach, and direction. Thus, even though a fork is based on its parent software's source code, it is a new and independent project in its own right. Because it is hard to legally secure the rights to a propriety software source code, forking occurs almost exclusively within the free software development world. This type of software's "open source" nature also means that any user is within their rights to use, study, change, and distribute both it and its source code. [Exhibit 78, p. 2]

³⁵ (U) According to an August 18, 2020 CoinTelegraph article accessed on October 3, 2020, crypto offramps are a way to convert your cryptocurrency into fiat [currency]. [Exhibit 193, p. 4]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

B. (U) **TORNADO CASH**

(U) As will be detailed below, **TORNADO CASH** is an entity^{36, 37} that provides cryptocurrency mixing services. OFAC assesses that **TORNADO CASH** is an entity — that is, a “partnership, association, trust, joint venture, corporation, group, subgroup, or other organization” — that may be designated pursuant to the International Emergency Economic Powers Act, 50 U.S.C. §§ 1701-1708 (IEEPA). See section 6(b), E.O. 13694, as amended; section 9(b), E.O. 13722.

TORNADO CASH’s organizational structure consists of: (1) its founders — Alexey Pertsev, Roman Semenov, and Roman Storm — and other associated developers, who together launched the Tornado Cash mixing service, developed new Tornado Cash mixing service features, created the **TORNADO CASH** Decentralized Autonomous Organization (DAO), and actively promote the platform’s popularity in an attempt to increase its user base; and (2) the DAO, which is responsible for voting on and implementing new features created by the developers. In order to participate in the **TORNADO CASH** DAO, members must obtain “TORN,” a virtual token issued by **TORNADO CASH** that gives the holder the right to vote on governance measures and influence the ongoing development and maintenance of the service operated by **TORNADO CASH**. Although TORN plays an important governance function, it is also a virtual currency that may be bought and sold on secondary markets, the value of which increases as **TORNADO CASH** increases its user base and popularity. **TORNADO CASH** uses computer code known as “smart contracts” to implement its governance structure, provide mixing services, offer financial incentives for users, increase its user base, and facilitate the financial gain of its users and developers.

(U//~~FOUO~~) **TORNADO CASH** collects fees through its “relayers,” which provide a widely used, anonymity-enhancing service for users. In order for a relayer to be listed on the Tornado Cash relayer registry, the relayer must “stake” (i.e., deposit) TORN, the **TORNADO CASH** DAO’s governance token. **TORNADO CASH** collects a fee from relayers for each transaction processed by the relayer, and distributes those fees to members of the **TORNADO CASH** DAO. The relayers, in turn, collect a fee from users of **TORNADO CASH**.

(U//~~FOUO~~) Specifically, an Ethereum transaction processed by **TORNADO CASH** through a relayer involves several fees:

1. The Ethereum “gas” fee, which is the fee paid in Ethereum by the initiator of any transaction on the Ethereum network to the validators who process the transactions.
2. The fee paid by the Tornado Cash user to the relayer, which is deducted from the funds deposited by the user to the Tornado Cash smart contract. In the case of an Ethereum transaction, this fee would be paid in Ethereum.
3. The fee paid by the relayer to **TORNADO CASH**, which is paid in TORN and deducted from the TORN that the relayer staked to be listed as an available relayer by **TORNADO CASH**. These TORN fees are distributed to members of the DAO who have staked their TORN to vote on **TORNADO CASH** governance proposals. This voting process is

³⁶ (U) E.O. 13694, as amended, defines an entity as a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization. [Exhibit 99, p. 2]

³⁷ (U) E.O. 13722 defines an entity as a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization. [Exhibit 100, p. 5]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

further described in *Section IV.B.2, (TORNADO CASH: Decentralized Autonomous Organization (DAO))*.

(U//~~FOUO~~) Relayers are more fully described in *Section IV.C.4 (The Tornado Cash Mixing Service: The Relayer Network)*.

1. (U) **TORNADO CASH: Founders and Developers**

(U)

[Exhibit 3, p. 1]

(U) According to a January 25, 2022 CoinDesk article, in an interview with CoinDesk, Tornado Cash co-founder Roman Semenov said, “The Tornado Cash team mostly does research and publishes the code to GitHub.^{38, 39} All the deployments, protocol changes, and important decisions are made by the community via Tornado Governance Decentralized Autonomous Organization and deployment ceremonies,” which are events when new code is pushed live. [Exhibit 6, pp. 3–4]

(U) According to the employment opportunity page on **TORNADO CASH**’s website, **TORNADO CASH** had an open job advertisement that states that it is “looking for a Solidity⁴⁰ Engineer, to join our ranks and strengthen our skill set.” The advertisement states that hires will:

- Design and write smart contracts on Ethereum to implement new features;
- Collaborate and share experiences with an enthusiastic and driven team;
- Contribute integrating state-of-the-art features for the next version of the protocol;
- Work in a fast-paced and challenging environment;
- Be able to work autonomously, great communication remotely, and continually get self-connected; and

³⁸ (U) According to its website, GitHub offers free and paid products for storing and collaborating on code. Some products apply only to personal accounts, while other plans apply only to organization and enterprise accounts. [Exhibit 80, p. 1]

³⁹ According to the website of the General Services Administration, accessed on October 24, 2022, GitHub is a web-based interface that uses Git, the open-source version control software that lets multiple people make separate changes to web pages at the same time. GitHub allows multiple developers to work on a single project at the same time, reduces the risk of duplicative or conflicting work, and can help decrease production time. With GitHub, developers can build code, track changes, and innovate solutions to problems that might arise during the site development process simultaneously. Non-developers can also use it to create, edit, and update website content. [Exhibit 219, pp. 1–2]

⁴⁰ (U) According to an article on Ethereum’s website, last updated on February 15, 2022, Solidity is a programming language for implementing smart contracts. [Exhibit 118, p. 1]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

- If interested, gain significant knowledge on zk-SNARKs⁴¹ and improve your skills on this topic.” [Exhibit 119, p. 1]

(U) According to an August 15, 2022 Cointelegraph article, in 2021, **TORNADO CASH** created a fund to provide incentives to key contributors to the project.⁴² [Exhibit 18, pp. 1–2]

(U) According to the GitHub page of the archived code base of the software used by **TORNADO CASH**, the source code contains 34 different repositories.⁴³ [Exhibit 48, p. 1]

(U) According to the commit log for the “Tornado Core” repository, the most recent commit⁴⁴ was by user “Alexey Pertsev” on March 24, 2022. Another commit was by user “Roman Semenov” on October 31, 2021. Still another commit was by user “poma”⁴⁵ on October 29, 2021. [Exhibit 74, p. 1] OFAC assesses that the usernames “Alexey Pertsev” and “Roman Semenov” are associated with **TORNADO CASH** developers Alexey Pertsev and Roman Semenov. Additional information regarding these individuals is discussed in *Section IV.E.2*.

(U//~~FOUO~~) Based on the above information regarding the “Tornado Core” commit log, OFAC concludes that the software used and developed by **TORNADO CASH** has undergone active development by a core group of developers over a period of multiple years.

2. (U) **TORNADO CASH: Decentralized Autonomous Organization (DAO)**

⁴¹ (U) According to the “What are zk-SNARKs?” page of the Zcash website, [REDACTED] “zk-SNARK” stands for “Zero-Knowledge Succinct Non-Interactive Argument of Knowledge,” and refers to a proof of construction where one can prove possession of certain information, e.g. a secret key, without revealing that information, and without any interaction between the prover and verifier. [Exhibit 133, p. 1]

⁴² (U) According to the August 15, 2022 Cointelegraph article, accessed on August 25, 2022, “the fund was held in a community-managed multi-signature wallet with five peer-elected members validating transactions who were selected because of their contributions to the project. Following the United States’ sanctioning of USD Coin (USDC) and Ethereum addresses associated with the crypto mixer Tornado Cash, the signatories of the projects’ multi-signature community fund have disbanded.” “However, given that interacting with Tornado Cash now comes with more risks — including penalties for U.S. citizens ranging from fines of up to \$10 million to prison time of up to 30 years — the community members in charge of the fund have vacated their posts and handed control to the project’s DAO. On August 12, the signatories started to relinquish their ability to manage the fund. On August 12, [2022], the signatories started to relinquish their ability to manage the fund. And on August 14, 2022 all five members of the multi-signature wallet completely removed their access, leaving only the governance wallet as the fund’s sole owner.” [Exhibit 18, p. 2]

⁴³ (U) According to the website of GitHub, [REDACTED] a repository is usually used to organize a single project. Repositories can contain folders and files, images, videos, spreadsheets, and data sets, anything your project needs. Often, repositories include a README file, a file with information about your project. [Exhibit 229, p. 2]

⁴⁴ (U) According to the website of GitHub, you can save small groups of meaningful changes as *commits*. Similar to saving a file that has been edited, a *commit* records changes to one or more files in your branch. [Exhibit 80, p. 1]

⁴⁵ (U//~~FOUO~~) A GitHub user profile page for “poma” [REDACTED] links to the **TORNADO CASH** website and lists the user’s real name as “Roman Semenov.” [Exhibit 208, p. 1] Based on this information, OFAC assesses that the username “poma” was also controlled by **TORNADO CASH** founder Roman Semenov.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

(U) **TORNADO CASH** is controlled by a DAO, which is comprised of members who have obtained TORN⁴⁶ tokens. TORN tokens provide members of the DAO with ownership stake in a fashion similar to stockholders; the more TORN tokens a member has, the more voting power they have. Developers of **TORNADO CASH** research and develop new features to **TORNADO CASH** and post them on websites such as GitHub for members of the DAO to propose to the collective members of the DAO for implementation. If a vote to implement passes, the DAO implements the new features in a process called Trusted Setup Ceremony. The DAO is the central controlling mechanism of **TORNADO CASH**.

a. (U) *The TORN Token*

(U) **TORNADO CASH** governance is accomplished through the DAO, which is made up of individuals who have been issued TORN tokens. According to a September 6, 2021 blog post on the website of Medium,⁴⁷ authored by **TORNADO CASH**, which has since been deleted by the author, and which was accessed by OFAC through the Wayback Machine's August 8, 2022 archive, the blog post describes the **TORNADO CASH** decision making processes, which combines both on-chain⁴⁸ and off-chain⁴⁹ governance:

“Governance is at the heart of every decentralized protocol and Tornado Cash does not deviate from this rule. By principle, for a decentralized protocol to function correctly, the decision-making process needs to be put between the hands of its users. Those users form a community that has the right & duty to shape the next versions of the tool they use. Usually, this community has the means to express itself through governance tokens. In other words, if the protocol was the community's battlefield, governance would be its weapon & tokens its ammunition. For the DAO to run smoothly, governance rules need to be clearly specified and cover all potential areas. We just need to take a look at political voting systems around the world to assert that decision making rules have a tremendous impact on the final made decision. On-chain governance offers the community (i.e., TORN holders) the means to implement the desired changes to their protocol. If the community agrees on adding or changing a given feature, the update will only be implemented if the on-chain governance rules are complied with. All those changes must go through proposals. Those proposals can be suggested to Tornado Cash users & TORN holders directly on <https://app.tornado.cash/governance> [the Tornado Cash Website], by any eligible community [i.e., DAO] member.” [Exhibit 70, pp. 2–4]

⁴⁶ (U) According to an August 13, 2022 Bitcoin.com article, TORN is the Tornado Cash governance token with a fixed supply, and which may be used to propose changes to Tornado Cash and its governance, and vote on such changes. There are approximately 1,511,065 TORN tokens, with 30 percent reserved for the developers and contributors. [Exhibit 34, p. 1]

⁴⁷ (U) According to the “About” page of its website, accessed on April 22, 2022, Medium is an open platform where over 100 million readers come to find insightful and dynamic thinking, where expert and undiscovered voices alike dive into the heart of any topic. [Exhibit 41, p. 1]

⁴⁸ (U) According to an October 2018 NIST report, “on-chain” refers to data that is stored or a process that is implemented and executed within a blockchain system. [Exhibit 189, p. 82]

⁴⁹ (U) According to an October 2018 NIST report, “off-chain” refers to data that is stored or a process that is implemented and executed outside of any blockchain system. [Exhibit 189, p. 82]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

(U) According to the website^{50, 51} of **TORNADO CASH** written by the “Tornado Team” and accessed through the Wayback Machine’s June 17, 2022 archive, TORN is an ERC-20-compatible token with a fixed supply that governs **TORNADO CASH**. TORN holders can make proposals and vote to change the protocol via governance. **TORNADO CASH** asserts that TORN is not a fundraising device or investment opportunity. It also indicates that the initial distribution of TORN was broken down as follows:

- 5% (500,000 TORN): Airdrop⁵² to early users of Tornado Cash ETH pools;⁵³
- 10% (1,000,000 TORN): Anonymity mining⁵⁴ for Tornado Cash ETH pools, distributed linearly over one year;
- 55% (5,500,000 TORN): DAO treasury,⁵⁵ will be unlocked linearly over five years with three-month cliff;⁵⁶
- 30% (3,000,000 TORN): Founding developers and early supporters, will be unlocked linearly over three years with one year cliff. [Exhibit 4, p. 1]

⁵⁰ (U) Following OFAC’s August 8, 2022 designation of **TORNADO CASH**, the website “Tornado.Cash” was shut down and is no longer accessible, except through the Internet Archive.

⁵¹ (U) According to its website, the Internet Archive, a 501(c)(3) non-profit, is building a digital library of Internet sites and other cultural artifacts in digital form. Like a paper library, it provides free access to researchers, historians, scholars, people with print disabilities, and the general public. Its mission is to provide “Universal Access to All Knowledge.” [Exhibit 20, p. 1]

⁵² (U) According to Cointelegraph, airdrops are a marketing strategy used by startups to give tokens to existing cryptocurrency traders for free or in exchange for minimal promotional work. [Exhibit 22, p. 1]

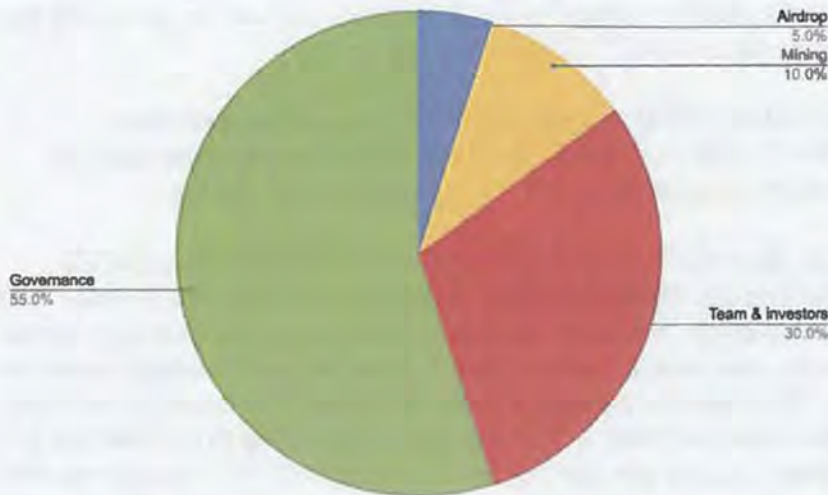
⁵³ (U//~~FOUO~~) Based on the context in which the term is used in this exhibit, OFAC assesses that “pools” refers to liquidity pools. According to a June 7, 2022 CoinDesk article, a liquidity pool is a digital pile of cryptocurrency locked in a smart contract. This results in creating liquidity for faster transactions. [Exhibit 220, p. 2]

⁵⁴ (U) Anonymity Mining is explained in more detail in *Section IV.C.3 (The Tornado Cash Mixing Service: Anonymity Mining)*.

⁵⁵ (U) The DAO Treasury is explained in more detail in *Section IV.B.2.b (TORNADO CASH: Decentralized Autonomous Organization (DAO))*

⁵⁶ (U) According to a December 9, 2021 post on Medium, cliffs are known as the period of time that must pass before the release of tokens starts. The duration of the cliffs can vary depending on the purpose of an allocation. Methods like cliffs (also known as “lock-up” periods) and vesting emerge as a means of aligning the interests of all participants and earning the trust of investors. [Exhibit 69, pp. 1–2]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~



[Exhibit 4, pp. 1–2]

(U) According to **TORNADO CASH’s** website, accessed through the Wayback Machine’s April 20, 2022 archive, “since its inception, the TORN token has been used by Tornado Cash users for governance. Its main utility is to allow the suggestion of proposals and voting both on-chain (through locked TORN for governance proposals) and off-chain (on Snapshot).⁵⁷ Since the execution of Tornado Cash’s tenth governance proposal, TORN token[s] ha[ve] gained one other useful utility. Indeed, with the introduction of a decentralized relayer register, a staking⁵⁸ reward has been implemented for all holders with locked TORN in the governance contract. TORN holders can still lock their tokens into the governance contract as they used to for governance purposes. The significant difference is that they are now able to receive a portion of the fees collected by the protocol from relayers. Obviously, the proportion of the reward will be equal to the proportion of their locked TORN. The collection of these fees was made possible by the implementation of a decentralized relayer registry. To be listed on the protocol user interface (UI),⁵⁹ relayers need to stake a given amount of TORN (currently set by governance at 300 TORN) and keep enough TORN locked (~40 TORN at the moment in April 2022) to be able to pay back the transaction fee to the staking contract. In a nutshell, for each withdrawal through

⁵⁷ (U) Snapshot is a centralized voting system. It provides flexibility on how voting power is calculated for a vote. Snapshot supports various voting option types to cater the needs of organizations. Creating proposals and voting on Snapshots is user-friendly and does not cost gas as the process is performed off-chain. [Exhibit 67, p. 1]

⁵⁸ (U) According to Cointelegraph, staking refers to a strategy where one can invest in a stake pool with a fraction of the number of tokens required to become a validator on a blockchain, while the staking pool rewards users on a daily, weekly or quarterly basis, depending on the cryptocurrency being staked. [Exhibit 25, p. 4] Staking Pools allow people to join other crypto investors to raise staking capital. Participants can then deposit any amount of tokens to a staking pool and start earning passive income proportional to the amount on their holdings. [Exhibit 49, p. 3]

⁵⁹ (U) According to the website of TechTarget, UI is the point of human-computer interaction and communication in a device. [Exhibit 16, p. 1]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

the relayer method, the chosen relayer has to pay a fee to the protocol⁶⁰ from the staked balance. Currently,⁶¹ this fee has been fixed at 0.3 percent by the governance and can be changed at any time through an on-chain proposal and vote.” [Exhibit 5, p. 1]

(U//~~FOUO~~) Although **TORNADO CASH** asserted that TORN was not an investment opportunity, as detailed below, TORN has been identified as an investment opportunity by multiple sources due to its ability to generate returns through trading and staking.

(U) According to an April 30, 2022 Medium post by PowerPool,⁶² “TORN is the ERC-20 governance token used in the Tornado Cash ecosystem. Recently, the TORN tokenomics⁶³ were updated, and now, TORN Relayers pay protocol TORN fees to the governance staking contract. Thus, TORN has three primary use-cases, (1) governance — it can be used to create proposals and to participate in voting; (2) it captures Tornado.Cash protocol fees; (3) it incentivizes user participation since it distributes protocol fees to TORN stakers. According to the Medium post, PowerPool announced ppTORN, a vault that allows users to maximize TORN staking returns thanks to PowerPool’s auto-compounding algorithm. PowerPool states that ppTORN is a smart contract that aggregates user deposits into the Tornado Cash governance staking contract. The ppTORN vault harvests and auto-compounds TORN rewards (protocol fees); ppTORN uses a smart algorithm for harvesting and re-staking which allows it to compound the rewards for Tornado token holders while reducing overall gas costs.” [Exhibit 143, pp. 1–3]

(U) According to a February 9, 2021 BTC Geek⁶⁴ article, **TORNADO CASH** “has been in operation for a while now and has proven its effectiveness in real-world adversarial scenarios. To that end, the protocol has come up with its own token, TORN. This is currently a governance-only token but it is not hard to see how it can become a value capture token via fees. The users of [**TORNADO CASH**] would not mind paying some fees for peace of mind and privacy. TORN’s tokenomics is well thought out and the inflation schedule is very gradual with no bumpy lockups expiring. In addition, there are no pesky VCs⁶⁵ in TORN’s allocation ready to dump on retail as soon as possible and bring down its value. The allocation of TORN has been very fair, providing TORN to early users of the Tornado protocol and using TORN as an

⁶⁰ (U//~~FOUO~~) Based on the context in which this information is presented, OFAC assesses that “protocol,” as used in this context, is a reference to the Tornado Cash Governance Contract.

⁶¹ (U//~~FOUO~~) Given that April 2022 is referenced previously in this exhibit, OFAC assesses that “currently,” as used here, refers to on or about April 2022.

⁶² (U) According to the Medium post, PowerPool DAO manages a growing range of structured DeFi products. PowerPool DAO’s mission is to create and actively manage a broadly diversified portfolio of automated, gas/capital-efficient, structured DeFi product portfolios deployed across EVM-compatible networks, with 100% of management fees accruing to the xCVP stakers controlling the DAO. [Exhibit 143, p. 3]

⁶³ (U) According to CoinDesk, tokenomics is a catch-all for the elements that make a particular cryptocurrency valuable and interesting to investors. That includes everything from a token’s supply and how it’s issued to things like what utility it has. [Exhibit 1, p. 2]

⁶⁴ (U) According to its website, BTC Geek is a blog and journalistic resource that caters to the Bitcoin and crypto community and publishes everything from news to opinion. [Exhibit 12, p. 1]

⁶⁵ (U//~~FOUO~~) According to Cointelegraph, the crypto industry is maturing fast, with many quick to compare it to the gold rush. And with industry maturity, users are beginning to witness a flood of traditional and retail investors flocking to the crypto space. Venture capital funds and other institutional investors are increasingly eyeing cryptocurrency businesses to see if there’s a profit to be made in financing them. [Exhibit 188, p. 1] OFAC assesses “VC,” as used here, is a reference to venture capital.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

incentive mechanism to increase the number of users and total value locked (TVL)⁶⁶ in the protocol. This is essential to the success of TORN and Tornado since the larger the anonymity set, the better it is for the users. You can also farm⁶⁷ TORN instead of buying TORN from an exchange. This is a long-term play since the amount of TORN that you earn depends on the time you are staked. However, this is good because TORN is gradually released into the market.” [Exhibit 142, pp. 1–3]

(U) According to a May 11, 2022 article on the website of AltCoinBuzz,⁶⁸ DeFi earnings platform PowerPool has announced a new vault for the Tornado Cash token, TORN. The protocol made the announcement that the ppTORN pool was live on May 10, 2022. According to the announcement, the team calculated that during a two-month period, users generated 61 percent APY⁶⁹ in the ppTORN vault. This is better than the 52 percent they earned for direct staking without the vault. There was almost \$100,000 in total value locked in the vault at the time of writing. [Exhibit 144, pp. 1–2]

(U) According to a March 5, 2022 Crypto News Australia⁷⁰ article, TORN surged 94 percent following the launch of its latest network updates. The latest price action for TORN follows the adoption and implementation of the protocol’s tenth on-chain governance proposal, which saw the addition of relayers to the network. The community voted overwhelmingly in favor of the proposal, which was accepted on February 19, 2022. Following the launch of the relayers on March 2, 2022. The price of TORN spiked from around \$37 to around the \$67 mark. [Exhibit 176, pp. 2–3]

(U) According to a January 25, 2022 CoinDesk article, in an interview with CoinDesk, **TORNADO CASH** co-founder Roman Semenov said, “The Tornado Cash team mostly does research and publishes the code to GitHub. All the deployments, protocol changes, and important decisions are made by the community via Tornado Governance⁷¹ [DAO] and deployment ceremonies,” an event when new code is pushed live. [Exhibit 6, pp. 3–4]

(U) According to the “FAQ” page of **TORNADO CASH**’s website [REDACTED] “the governance of Tornado Cash is completely decentralized, controlled, and governed by its

⁶⁶ (U) According to a January 27, 2022 CoinDesk article, TVL is the overall value of crypto assets deposited in a DeFi protocol or in DeFi protocols generally. It has emerged as a key metric for gauging interest in that particular sector of the crypto industry. TVL includes all the coins deposited in all of the functions that DeFi protocols offer, including staking, lending, and liquidity pools. [Exhibit 173, p. 2]

⁶⁷ (U//~~FOUO~~) OFAC assesses that this is a reference to Anonymity Mining.

⁶⁸ (U) According to its website, AltCoinBuzz is an independent digital media outlet that delivers the latest news and opinions in the world of Cryptocurrencies, Blockchain Technology, Regulations, Adoption and Blockchain Gaming. [Exhibit 40, p. 1]

⁶⁹ (U) According to the website of CoinMarketCap, APY is the rate of return gained over the course of a year on a specific investment. [Exhibit 105, p. 1]

⁷⁰ (U) According to its website, Crypto News was founded in 2017 as an online publication where readers can find independent news in relation to cryptocurrencies and blockchain. [Exhibit 172, p. 1]

⁷¹ (U//~~FOUO~~) According to a page on the website of Ethereum titled “Introduction to Ethereum governance,” governance is the systems in place that allow decisions to be made: “In a typical organizational structure, the executive team or a board of directors may have the final say in decision-making. Or perhaps shareholders vote on proposals to enact change. In a political system, elected officials may enact legislation that attempts to represent their constituents’ desires. [Exhibit 50, p. 1]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

DAO. By acquiring TORN tokens, customers can participate by voting on governance proposals.” [Exhibit 160, p. 2]

(U) According to an August 12, 2022 Decrypt⁷² article, the Tornado Cash TORN token is used by the Tornado Cash DAO to manage governance and voting. [Exhibit 7, p. 2]

(U) According to the website of **TORNADO CASH**, accessed through the Wayback Machine’s August 5, 2022 archive, thanks to the TORN token, protocol parameters and token distribution are completely under the community’s control. [Exhibit 120, p. 3]

(U) According to the same September 6, 2021 Medium post, authored by “Tornado Cash,” “to sum-up Tornado Cash governance rules:

- TORN tokens need to be locked⁷³ in the Tornado Cash governance contract to get used for governance & cannot be unlocked until the end of the proposal;
- A minimum of 1,000 locked TORN is needed to create a proposal on the [Tornado Cash app];
- Community members have a time-lapse of 3 days to vote with their locked TORN; A proposal is executed if:
 - (i) a 25,000 TORN quorum is reached, [and]
 - (ii) the number of TORN vouching for the proposal exceeds the number of TORN that are against it;
- Changes agreed on through those governance rules are binding, which means that any user can deploy them after a two-days time-lock and within a period of 3 days.” [Exhibit 70, pp. 3–4]

(U) According to the same September 6, 2021 blog post on the website of Medium, on-chain governance helps maintain transparency as rules are clearly specified and known by the whole community. “It also enables changes and updates to get implemented in a decentralized environment where users are the actual stakeholders of the protocol. When the power lies in the hands of many individuals, decision making rules are crucial. This is especially true since those binding changes are directly deployed on the Blockchain and impact the functioning of the whole protocol. A wise man once said: with great power comes great responsibility. However, all decisions made by the community don’t need to go through strict on-chain governance guidelines, locked tokens in contracts and Tornado Cash proposals system. Indeed, proposals can only concern specific areas such as changing reward parameters for Anonymity Points or changing certain core mining contracts. A lot of decisions, such as the use of the Tornado Cash Community Fund or the election of its multi-signature key holders, are made through off-chain governance.”⁷⁴ [Exhibit 70, p. 4]

⁷² (U) According to its website, Decrypt was founded in 2018 with a simple mission: to demystify the decentralized web. [Exhibit 196, p. 1]

⁷³ (U) According to the website of Binance, [REDACTED] the term token lockup refers to a specific period of time in which cryptocurrency tokens cannot be transacted or traded. Typically, these lockups are used as a preventive strategy to maintain a stable long-term value of a particular asset. [Exhibit 194, p. 1]

⁷⁴ (U) According to the encyclopedia section of the website of PCMag, accessed on October 24, 2022, off-chain governance is a blockchain that operates like any organization, wherein a core group of people make decisions. For

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

(U) According to a February 9, 2021 Coin Telegraph article, “[DeFi] ‘stimulus checks’ keep coming as Tornado Cash joins Uniswap, Badger DAO, StakeDAO, and others in “airdropping” a now-tradable TORN governance token to early protocol participants. Tornado Cash, which is an Ethereum “tumbling” service that obscures transactional history in order to preserve user privacy (as well as allow scammers and hackers a method to launder their funds), first announced the launch of a governance token in December. A snapshot for the airdrop was taken for Ethereum block 11400000, which was mined on December 6th, 2020⁷⁵ and addresses which had interacted with the protocol prior to that point were entitled to an amount of TORN tokens weighted to the frequency and amount of Ether they used. At current valuations, the distribution was one of the most lucrative for recipients to date. According to a post on community forums, the average recipient received 66.54 TORN tokens currently worth over \$23,000, and the median user took in 21.24 tokens, worth \$7500. The single largest recipient harvested over 2500 tokens worth a whopping \$888,000. The 500,000 airdropped tokens represent just 5 percent of the eventual 10,000,000 total TORN supply.” [Exhibit 121, pp. 1–2]

b. (U) Community Fund

(U) According to the website of **TORNADO CASH**, accessed through the Wayback Machine’s June 17, 2022 archive, in June 2021, “to help build future enhanced versions of Tornado Cash, all skills and talents are well welcomed. Involvement opportunities are almost unlimited. Those opportunities involve any function or contribution that improves the protocol and its position within the blockchain ecosystem. The Tornado Cash community is looking for:

- Developers that can help continue building the protocol and its tools;
- Auditors who can review code to find bugs and vulnerabilities;
- Content creators in order to make educational or promotional content to attract new users to the protocol (videos, blogs, memes, etc.); and
- Potential hires for the DAO.” [Exhibit 122, p. 1]

(U) According to the website of **TORNADO CASH**, accessed through the Wayback Machine’s June 17, 2022 archive, “in June 2021, [the] Tornado.Cash community⁷⁶ has voted the implementation of a community fund to reward its key contributors. The management of this fund lies with the community. Tornado.Cash users are the ones who decide whose contribution is eligible for a compensation. Tornado.Cash Community Fund has been allocated 5% of total available TORN of the governance treasury, broken down as follows:

- 5% of the already vested 485,300 TORN at that time, resulting on an initial transfer of 22.9 thousand TORN.

example, Bitcoin and Ethereum use off-chain governance. In contrast, on-chain governance is how a DAO operates. DAOs issue governance tokens, and members have voting rights because they purchased or were given voting tokens. [Exhibit 223, p. 1] According to its website, accessed on October 25, 2022, PCMagazine delivers lab-based, independent reviews of the latest products and services. [Exhibit 224, p. 1]

⁷⁵ (U) According to the website of Etherscan, [REDACTED] Ethereum block 11400000 occurred on December 6, 2020. [Exhibit 201, p. 1]

⁷⁶ (U//FOUO) Based on additional context provided in Exhibit 122, OFAC assesses that management of the community fund has included both control by the DAO and control by individuals selected to represent **TORNADO CASH**.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

- 5% of the monthly 91,600 [TORN] that will be vested in the next 12 months, which result on a monthly transfer of approximately 4,600 TORN.” [Exhibit 122, p. 2]

(U) According to the website of **TORNADO CASH**, accessed through the Wayback Machine’s June 17, 2022 archive, the monthly allocation of the Fund was programmed through Sablier, a protocol build on Ethereum that allows a live stream of remaining TORNs (second by second) over 12 months. In total, an amount of approximately 78,000 TORN was allocated to this Community Fund. As of the end of August 2021, the balance of the Community Fund is about 12,600 TORN vested in Sablier and 15,500 TORN in the gnosis safe. As of the beginning of 2022, the Community Fund (on Gnosis Safe) balance amounts to 36,400 TORN. Tornado.Cash Community Contract is 0xb04E030140b30C27bcdfaaffFA98C57d80eDa7B4. Funds are handled through a Multi-signature Wallet on Gnosis Safe. Keys to manage this wallet were put between the hand of 5 peer-elected community members. To validate a transaction, a consensus of 4-of-5 signatures is needed. Those multi-signatures key holders were chosen for their contribution & commitment to Tornado.Cash and its Community. They pledged to sign off transaction[s] following the community instructions. Those guidelines are expressed through forum discussion and corroborated by a Snapshot vote. All signers also pledged to resign if they no longer fulfill their allegiance to Tornado’s prosperity. They can also be dismissed from their role under the decision of the community. To reward their commitment as signers & key contributors for Tornado.Cash community, a minimum of 100 TORN per month per signer has been deployed through Sablier. The current 5 multi-signatures key holders are:

- 0xd26BaA5F41CC7839CEdb020b6d98E1C6e1642D75
- 0x7c09bCa28ba3DB1CF7cd793696B161261cAC27b5
- 0x339B45fBEed1ab46Fe9c11f484b0Ea7220e75300
- 0x647e9e26DA82C29AAfbbFB1C3f45d916AA9b300d
- 0xEA27752f7D6687CB3Be2F180B997713b784c9911 [Exhibit 122, pp. 2–3]

(U) According to the website of **TORNADO CASH**, accessed through the Wayback Machine’s June 17, 2022 archive, “multi-signature wallet, members of the community have “the ability to ask the community for compensation from this fund to reward his/her contribution to Tornado.Cash. Each member also has the ability to request compensation on behalf of another member to reward him/her for his/her work. To this extent, a new category titled «Funding» has been created on [the] Tornado.Cash discussion forum. By creating a new post in the category, all members can open a funding request to use the Community Fund. Discussions regarding terms and conditions of such a request are discussed on this post. Once these terms and conditions are fixed, a vote is conducted on Snapshot to validate (or not) such a funding request.” [Exhibit 122, p. 3]

(U) According to the website of **TORNADO CASH**, accessed through the Wayback Machine’s June 17, 2022 archive, “each specific funding request is accompanied by a Snapshot vote, where TORN holders can explicitly express their position. In order to vote on Snapshot, the community member needs to:

- Connect the wallet holding TORNs using MetaMask, WalletConnect, or Torus;
- Cast the vote, by either clicking on Accept or Refuse; and
- Confirm the vote.” [Exhibit 122, pp. 4–6]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

(U) According to an August 12, 2022 Theblock.co article, accessed November 5, 2022, “the Tornado Cash DAO community has voted in favor of adding the DAO’s governance as a signatory to the treasury’s multi-signatory (multisig) wallet. The Treasury looks after about \$21.6 million across three different wallets. This vote began on Wednesday, based on a proposal on the Tornado Cash DAO governance page, and ended today with 100% approval from all 12 participants. These 12 participants contributed 51,000 TORN tokens to push the vote to completion. The voting process was hastily put together with the SnapShot initiated together with the proposal. Usually, there is a delay between a proposal being filed and the commencement on-chain. This lag is to create adequate time for the community to discuss the matter at hand. But it would have taken too long for the DAO. “As it is very important, we need to move fast on this subject. I will make a snapshot vote today so you guys can vote on it during 3 days,” said the Tornado Cash DAO member who filed the proposal. With the vote passed, the DAO’s treasury will now become a four-of-six multisig instead of the previous four-of-five multi-sig arrangement. The Tornado Cash DAO governance will now be added as a signatory to the treasury wallet. Multisig wallets require a specific minimum number of signatories to approve a transaction. In this case, four out of the six signers must approve any transaction from the treasury. In practice, this means that if the core developers want to make a transaction involving the treasury, they will need to get signatures from at least four of the six multisig holders. Since one of these holders is now the DAO, they may need to ask the DAO to approve a signature. This would require the DAO to vote on whether to do so.” [Exhibit 204, pp. 1–3]

3. (U) **TORNADO CASH: Smart Contracts Associated with TORNADO CASH**

(U) According to an August 25, 2022 Coin Center article, each Tornado Cash pool is a smart contract deployed to Ethereum. Like other smart contracts, the pool contracts extend the functionality of Ethereum with specific operations that can be executed by any user of Ethereum according to the rules defined in the Tornado Cash contracts’ code. [Exhibit 62, p. 6]

(U//~~FOUO~~) According to the website of **TORNADO CASH**, accessed by the Wayback Machine’s June 17, 2022 archive, the Tornado Cash smart contracts include Tornado Cash Classic Pools Contracts,⁷⁷ Tornado Cash Nova Pool Contracts, Governance Contracts, Relayer Registry, and Other Contracts.⁷⁸ The smart contracts are as follows:

- (U) Tornado Cash Classic Contracts:
- I. 0x12D66f87A04A9E220743712cE6d9bB1B5616B8Fc
 - o Name: 0.1 ETH Pool Contract
 - II. 0x47CE0C6eD5B0Ce3d3A51fdb1C52DC66a7c3c2936
 - o Name: 1 ETH Pool Contract
 - III. 0x910Cbd523D972eb0a6f4cAe4618aD62622b39DbF

⁷⁷ (U) Each Tornado Cash pool takes deposits of a specific amount of a specific cryptocurrency.

⁷⁸ (U//~~FOUO~~) Although OFAC assesses that these smart contract addresses are associated with **TORNADO CASH**, OFAC was unable to confirm the accuracy of the labels assigned to the smart contracts by the **TORNADO CASH** website.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

- o Name: 10 ETH Pool Contract
- IV. 0xA160cdAB225685dA1d56aa342Ad8841c3b53f291
 - o Name: 100 ETH Pool Contract
- V. 0xD4B88Df4D29F5CedD6857912842cff3b20C8Cfa3
 - o Name: 100 DAI⁷⁹ Pool Contract
- VI. 0xFD8610d20aA15b7B2E3Be39B396a1bC3516c7144
 - o Name: 1,000 DAI Pool Contract
- VII. 0x07687e702b410Fa43f4cB4Af7FA097918ffD2730
 - o Name: 10,000 DAI Pool Contract
- VIII. 0x23773E65ed146A459791799d01336DB287f25334
 - o Name: 100,000 DAI Pool Contract
- IX. 0x22aaA7720ddd5388A3c0A3333430953C68f1849b
 - o Name: 5,000 cDAI⁸⁰ Pool Contract
- X. 0x03893a7c7463AE47D46bc7f091665f1893656003
 - o Name: 50,000 cDAI Pool Contract
- XI. 0x2717c5e28cf931547B621a5dddb772Ab6A35B701
 - o Name: 500,000 cDAI Pool Contract
- XII. 0xD21be7248e0197Ee08E0c20D4a96DEBdaC3D20Af
 - o Name: 5,000,000 cDAI Pool Contract
- XIII. 0x4736dCf1b7A3d580672CcE6E7c65cd5cc9cFBa9D
 - o Name: 100 USDC⁸¹ Pool Contract
- XIV. 0xd96f2B1c14Db8458374d9Aca76E26c3D18364307
 - o Name: 1,000 USDC Pool Contract
- XV. 0x169AD27A470D064DEDE56a2D3ff727986b15D52B
 - o Name: 100 USDT Pool Contract
- XVI. 0x0836222F2B2B24A3F36f98668Ed8F0B38D1a872f
 - o Name: 1,000 USDT Pool Contract
- XVII. 0x178169B423a011fff22B9e3F3abeA13414dDD0F1
 - o Name: 0.1 WBTC Pool Contract
- XVIII. 0x610B717796ad172B316836AC95a2ffad065CeaB4
 - o Name: 1 WBTC Pool Contract
- XIX. 0xbB93e510BbCD0B7beb5A853875f9eC60275CF498
 - o Name: 10 WBTC Pool Contract

⁷⁹ (U) According to the Blockchain Council, DAI is the first stable cryptocurrency that is decentralized and collateralized. It aims at reducing the volatility of trading on the blockchain. It is an ERC-20 token that ensures maintaining a value equal to one U.S. dollar. [Exhibit 51, p. 3]

⁸⁰ (U) According to a Decrypt article from April 20, 2020, cDAI is a Compound protocol token, which is a system of openly accessible smart contracts built on Ethereum. Compound focuses on allowing borrowers to take out loans and lenders to provide loans by locking their crypto assets into the protocol called cTokens. New cTokens are created whenever a user deposits crypto-assets into the Compound protocol. If users want to take out a loan using ETH as collateral, they automatically receive cETH in return for their deposited ETH. Anyone can mint or create cTokens using an Ethereum wallet such as MetaMask, Coinbase wallet, or Huobi wallet plus one of the crypto assets the Compound system currently accepts. As of December 2019, users of Compound could borrow or lend BAT, DAI, ETH, REP, USDC, WBTC, and ZRX. [Exhibit 52, p. 2]

⁸¹ (U) According to Investopedia, USD Coin (USDC) is a digital currency that is fully backed by U.S. dollar assets. USDC is a tokenized U.S. dollar, with the value of one USDC coin pegged 1:1 to the value of one U.S. dollar. The value of USDC is designed to remain stable, making USDC a stablecoin. [Exhibit 73, p. 1]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

- XX. 0x84443CFd09A48AF6eF360C6976C5392aC5023a1F
 - o Name: 0.1 ETH Pool Contract
- XXI. 0xd47438C816c9E7f2E2888E060936a499Af9582b3
 - o Name: 1 ETH Pool Contract
- XXII. 0x330bdFADE01eE9bF63C209Ee33102DD334618e0a
 - o Name: 10 ETH Pool Contract
- XXIII. 0x1E34A77868E19A6647b1f2F47B51ed72dEDE95DD
 - o Name: 100 ETH Pool Contract
- XXIV. 0xdf231d99Ff8b6c6CBF4E9B9a945CBACeF9339178
 - o Name: 1,000 xDAI⁸² Pool Contract
- XXV. 0xaf4c0B70B2Ea9FB7487C7CbB37aDa259579fe040
 - o Name: 10,000 xDAI Pool Contract
- XXVI. 0xa5C2254e4253490C54cef0a4347fddb8f75A4998
 - o Name: 100,000 xDAI Pool Contract
- XXVII. 0xaf8d1839c3c67cf571aa74B5c12398d4901147B3
 - o Name: 500 AVAX⁸³ Pool Contract
- XXVIII. 0x6Bf694a291DF3FeC1f7e69701E3ab6c592435Ae7
 - o Name: 0.1 ETH Pool Contract
- XXIX. 0x3aac1cC67c2ec5Db4eA850957b967Ba153aD6279
 - o Name: 1 ETH Pool Contract
- XXX. 0x723B78e67497E85279CB204544566F4dC5d2acA0
 - o Name: 10 ETH Pool Contract
- XXXI. 0x0E3A09dDA6B20aFbB34aC7cD4A6881493f3E7bf7
 - o Name: 100 ETH Pool Contract
- XXXII. 0x76D85B4C0Fc497EeCc38902397aC608000A06607
 - o Name: 100 DAI Pool Contract
- XXXIII. 0xCC84179FFD19A1627E79F8648d09e095252Bc418
 - o Name: 1,000 DAI Pool Contract
- XXXIV. 0xD5d6f8D9e784d0e26222ad3834500801a68D027D
 - o Name: 10,000 DAI Pool Contract
- XXXV. 0x407CcEeaA7c95d2FE2250Bf9F2c105aA7AAFB512
 - o Name: 100,000 cDAI Pool Contract
- XXXVI. 0x833481186f16Cece3f1Eee1a694c42034c3a0dB
 - o Name: 5,000 cDAI Pool Contract
- XXXVII. 0xd8D7DE3349ccaA0Fde6298fe6D7b7d0d34586193
 - o Name: 50,000 cDAI Pool Contract
- XXXVIII. 0x8281Aa6795aDE17C8973e1aedcA380258Bc124F9
 - o Name: 500,000 cDAI Pool Contract
- XXXIX. 0x57b2B8c82F065de8Ef5573f9730fC1449B403C9f
 - o Name: 5,000,000 cDAI Pool Contract

⁸² (U) According to a March 3, 2021 Medium article, the xDai chain is an Ethereum-based sidechain that uses a Proof-of-Stake mechanism. It has been live since late 2018 and uses a stablecoin, xDai, as its native cryptocurrency. [Exhibit 75, p. 1]

⁸³ (U) According to a September 16, 2022 Forbes article, Avalanche (AVAX) is a cryptocurrency and blockchain platform set up to rival Ethereum. Within the Avalanche blockchain, AVAX is used as the token to support a suite of blockchain projects, such as tracking smart contracts. [Exhibit 85, p. 2]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

- XL. 0x05E0b5B40B7b66098C2161A5EE11C5740A3A7C45
 - o Name: 100 USDC Pool Contract
- XLI. 0x23173fE8b96A4Ad8d2E17fB83EA5dcccCa1Ae52
 - o Name: 1,000 USDC Pool Contract
- XLII. 0x538Ab61E8A9fc1b2f93b3dd9011d662d89bE6FE6
 - o Name: 100 USDT⁸⁴ Pool Contract
- XLIII. 0x94Be88213a387E992Dd87DE56950a9aef34b9448
 - o Name: 1,000 USDT Pool Contract
- XLIV. 0x242654336ca2205714071898f67E254EB49ACdCe
 - o Name: 0.1 WBTC⁸⁵ Pool Contract
- XLV. 0x776198CCF446DFa168347089d7338879273172cF
 - o Name: 1 WBTC Pool Contract
- XLVI. 0xeDC5d01286f99A066559F60a585406f3878a033e
 - o Name: 10 WBTC Pool Contract

(U) Tornado Cash Nova Contracts:

- XLVII. 0xD692Fd2D0b2Fbd2e52CFa5B5b9424bC981C30696
 - o Name: Tornado Pool
- XLVIII. 0xca0840578f57fe71599d29375e16783424023357⁸⁶
 - o Name: L1 Omnibridge Helper
- XLIX. 0xDF3A408c53E5078af6e8fb2A85088D46Ee09A61b
 - o Name: Verifier 2
- L. 0x743494b60097A2230018079c02fe21a7B687EAA5
 - o Name: Verifier 16
- LI. 0x94C92F096437ab9958fC0A37F09348f30389Ae79
 - o Hasher / Poseidon 2

(U) Governance Contracts:

- LII. 0x5efda50f22d34F262c29268506C5Fa42cB56A1Ce
 - o Name: Governance Contract
- LIII. 0x2f50508a8a3d323b91336fa3ea6ae50e55f32185
 - o Name: Governance Vault (For Locked TORN)
- LIV. 0xCEe71753C9820f063b38FDdB4cFDAf1d3D928A80
 - o Name: Deployer Contract
- LV. 0xffbac21a641dcfe4552920138d90f3638b3c9fba
 - o Name: Governance Impl
- LVI. 0x179f48c78f57a3a78f0608cc9197b8972921d1d2
 - o Name: Governance Vesting

⁸⁴ (U) According to Investopedia, Tether (USDT) is a cryptocurrency stablecoin pegged to the U.S. dollar and backed "100% by Tether's reserves." [Exhibit 102, p. 1]

⁸⁵ (U) According to a May 17, 2022 Decrypt article, WBTC stands for Wrapped Bitcoin, an ERC-20 token that represents Bitcoin—one WBTC equals one BTC. A BTC can be converted into a WBTC and vice-versa. Being an ERC-20 token makes the transfer of WBTC faster than normal Bitcoin, but the key advantage of WBTC is its integration into the world of Ethereum wallets, decentralized apps (DApps), and smart contracts. [Exhibit 76, p. 2]

⁸⁶ (U) According to Coin Center, this smart contract allows users to designate deposited ETH to be bridged to a Tornado Cash pool located on the Gnosis Chain blockchain. [Exhibit 62, pp. 24–25]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

- LVII. 0xb04E030140b30C27bcdfaaffFA98C57d80eDa7B4
o Name: Community Fund
- LVIII. 0x77777feddddfc19ff86db637967013e6c6a116c
o Name: TORN Token
- LIX. 0x3efa30704d2b8bbac821307230376556cf8cc39e
o Name: Voucher TORN Token
- LX. 0x746aebc06d2ae31b71ac51429a19d54e797878e9
o Name: Mining v2
- (U) Relayer Registry Contracts:
- LXI. 0xd90e2f925DA726b50C4Ed8D0Fb90Ad053324F31b⁸⁷
o Name: Tornado Router
- LXII. 0x5f6c97C6AD7bdd0AE7E0Dd4ca33A4ED3fDabD4D7
o Name: Proxy of Fee Manager Contract
- LXIII. 0xf4B067dD14e95Bab89Be928c07Cb22E3c94E0DAA
o Name: FeeManager
- LXIV. 0x58E8dCC13BE9780fC42E8723D8EaD4CF46943dF2⁸⁸
o Name: Proxy of Relayer Registry Contract
- LXV. 0x01e2919679362dFBC9ee1644Ba9C6da6D6245BB1
o Name: Relayer Registry
- LXVI. 0x2FC93484614a34f26F7970CBB94615bA109BB4bf
o Name: Proxy of Staking Contract
- LXVII. 0x26903a5a198D571422b2b4EA08b56a37cbD68c89
o Name: Tornado Staking Rewards
- LXVIII. 0xB20c66C4DE72433F3cE747b58B86830c459CA911
o Name: Proxy of Instance Registry Contract
- LXIX. 0x2573BAc39EBE2901B4389CD468F2872cF7767FAF
o Name: Instance Registry
- (U) Other Contracts:
- LXX. 0x527653eA119F3E6a1F5BD18fbF4714081D7B31ce⁸⁹
o Name: Tornado.Cash Trees
- LXXI. 0x653477c392c16b0765603074f157314Cc4f40c32
o Name: Tree Update Verifier
- LXXII. 0x88fd245fEdeC4A936e700f9173454D1931B4C307
o Name: Reward Verifier
- LXXIII. 0x09193888b3f38C82dEdfda55259A82C0E7De875E
o Name: Withdraw Verifier
- LXXIV. 0x5cab7692D4E94096462119ab7bF57319726Eed2A
o Name: Reward Swap

⁸⁷ (U) According to Coin Center, this smart contract maintains a list of Tornado Cash pools, which can be used by users to route deposits and withdrawals to the correct Tornado Cash pool. [Exhibit 62, p. 24]

⁸⁸ (U) According to Coin Center, this smart contract allows anyone to register as a Tornado Cash Relayer. [Exhibit 62, p. 24]

⁸⁹ (U) According to Coin Center, this smart contract holds a merkle tree (a kind of list) of all Tornado Cash deposit and withdrawal events. [Exhibit 62, p. 24]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

- LXXV. 0x756C4628E57F7e7f8a459EC2752968360Cf4D1AA
o Name: Echoer
- LXXVI. 0x722122dF12D4e14e13Ac3b6895a86e84145b6967⁹⁰
o Name: Proxy
- LXXVII. 0x94A1B5CdB22c43faab4AbEb5c74999895464Ddaf⁹¹
o Name: Mixer 1
- LXXVIII. 0xb541fc07bC7619fD4062A54d96268525cBC6FfEF⁹²
o Name: Mixer 2
- LXXIX. 0xD82ed8786D7c69DC7e052F7A542AB047971E73d2
o Name: Poseidon 3
- LXXX. 0xDD4c48C0B24039969fC16D1cdF626eaB821d3384⁹³
o Name: Gitcoin Grants [Exhibit 177, pp. 1–9]

(U//~~FOUO~~) Etherscan⁹⁴ attributes the below smart contracts to **TORNADO CASH**. In addition, these smart contracts were deployed by address 0x8589427373D6D84E98730D7795D8f6f8731FDA16, which **TORNADO CASH** identified⁹⁵ as its donation address. Based on this, OFAC assesses that these addresses are associated with **TORNADO CASH**:

- I. 0xF67721A2D8F736E75a49FdD7FAd2e31D8676542a
o Name: Tornado.Cash: 10,000 USDT [Pool Contract]
o Contract Creator: Tornado.Cash: Donate
(0x8589427373D6D84E98730D7795D8f6f8731FDA16)
- II. 0x9AD122c22B14202B4490eDAf288FDb3C7cb3ff5E
o Name: Tornado.Cash: 100,000 USDT [Pool Contract]
o Contract Creator: Tornado.Cash: Donate
(0x8589427373D6D84E98730D7795D8f6f8731FDA16)
- III. 0xD691F27f38B395864Ea86CfC7253969B409c362d
o Name: Tornado.Cash 10,000 USDC [Pool Contract]
o Contract Creator: Tornado.Cash: Donate
(0x8589427373D6D84E98730D7795D8f6f8731FDA16)
- IV. 0xaEaaC358560e11f52454D997AAFF2c5731B6f8a6
o Name: Tornado.Cash: 5,000 cUSDC [Pool Contract]
o Contract Creator: Tornado.Cash: Donate
(0x8589427373D6D84E98730D7795D8f6f8731FDA16)
- V. 0x1356c899D8C9467C7f71C195612F8A395aBf2f0a
o Name: Tornado.Cash: 50,000 cUSDC [Pool Contract]

⁹⁰ (U) According to Coin Center, this smart contract is an old version of Tornado.Cash: Router. [Exhibit 62, p. 25]

⁹¹ (U) According to Coin Center, this smart contract is an old version of the Tornado Cash pools. [Exhibit 62, p. 26]

⁹² (U) According to Coin Center, this smart contract is an old version of the Tornado Cash pools. [Exhibit 62, p. 26]

⁹³ (U) According to Coin Center, this smart contract is used to receive software development grants from the Gitcoin crowdfunding platform. [Exhibit 62, p. 31]

⁹⁴ (U) According to its website, EtherScan is the leading BlockChain explorer, search, API, and Analytics Platform for Ethereum. [Exhibit 29, p. 1]

⁹⁵ (U) On August 23, 2019, **TORNADO CASH** tweeted: “Now you can donate to any Ethereum project anonymously. Just withdraw your note to donation address. Try it out with Tornado Cash donation address 0x8589427373D6D84E98730D7795D8f6f8731FDA16.” [Exhibit 195, p. 1]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

- Contract Creator: Tornado.Cash: Donate
(0x8589427373D6D84E98730D7795D8f6f8731FDA16)
 - VI. 0xA60C772958a3eD56c1F15dD055bA37AC8e523a0D
 - Name: Tornado.Cash: 500,000 cUSDC [Pool Contract]
 - Contract Creator: Tornado.Cash: Donate
(0x8589427373D6D84E98730D7795D8f6f8731FDA16)
 - VII. 0xBA214C1c1928a32Bffe790263E38B4Af9bFCD659
 - Name: Tornado.Cash: 50,000 cDAI [Pool Contract]
 - Contract Creator: Tornado.Cash: Donate
(0x8589427373D6D84E98730D7795D8f6f8731FDA16)
 - VIII. 0xb1C8094B234DcE6e03f10a5b673c1d8C69739A00
 - Name: Tornado.Cash: 500,000 cDAI [Pool Contract]
 - Contract Creator: Tornado.Cash Donate:
(0x8589427373D6D84E98730D7795D8f6f8731FDA16)
 - IX. 0xF60dD140cFf0706bAE9Cd734Ac3ae76AD9eBC32A
 - Name: Tornado.Cash: 10,000 DAI [Pool Contract]
 - Contract Creator: Tornado.Cash: Donate
(0x8589427373D6D84E98730D7795D8f6f8731FDA16)
- [Exhibit 101, pp. 2–10]

(U) According to the website of ImmuneFi,⁹⁶ accessed through the Wayback Machine's May 27, 2022 archive, **TORNADO CASH** had a bug bounty program⁹⁷ which was focused on its smart contracts and was focused on preventing:

- Thefts or freezing of funds in anonymity pools
- Thefts or freezing of unclaimed yield (TORN anonymity mining)
- Theft of governance funds (Main on-chain Tornado DAO treasury only)
- On chain governance activity disruption. [Exhibit 175, p. 2]

(U) According to the website of ImmuneFi, accessed through the Wayback Machine's May 27, 2022 archive, the Tornado Cash bug bounty program has fixed rewards in TORN. The maximum reward is capped at 32,500 TORN, which was the equivalent of \$1,300,000 at the time. [Exhibit 175, p. 3]

(U) According to the website of ImmuneFi, accessed through the Wayback Machine's May 27, 2022 archive, the following Tornado Cash smart contracts were in-scope for the Tornado Cash bug bounty program: 0.1 ETH pool, 1 ETH pool, 10 ETH pool, 100 ETH pool, 100 DAI pool, 1,000 DAI pool, 10,000 DAI pool, 100,000 DAI pool, 5,000 cDAI pool, 50,000 CdaI pool, 500,000 cDAI pool, 5,000,000 cDAI pool, 100 USDC pool, 1,000 USDC pool, 100

⁹⁶ (U) According to ImmuneFi's website, [REDACTED] founder and CEO Mitchell Amador launched ImmuneFi on December 9, 2020, as a bug bounty platform focused on web3 and smart contract security with the goal of making web3 safe for everyone. ImmuneFi provides bug bounty hosting, consultation, and program management services to blockchain and smart contract projects. [Exhibit 19, p. 1]

⁹⁷ (U) According to ImmuneFi's website, [REDACTED] bug bounty programs are open invitations to security researchers to discover and responsibly disclose vulnerabilities in projects' smart contracts and applications, which can save web3 projects hundreds of millions — and even billions — of dollars. For their good work, security researchers receive a reward based on the severity of the vulnerability. [Exhibit 19, p. 2]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

USDT pool, 1,000 USDT pool, 0.1 WBTC, 1 WBTC, 10 WBTC, TORN Token, Governance Proxy, Reward Verifier, Withdraw Verifier, Tree Update Verifier, Reward Swap, TornadoCash Proxy, TornadoTrees, Miner, and Poseidon Hasher. [Exhibit 175, pp. 5–12]

(U//~~FOUO~~) Based on the above description of the **TORNADO CASH** bug bounty program, OFAC assesses that **TORNADO CASH** offered TORN that it controlled to help identify and remediate security vulnerabilities in the Tornado Cash smart contracts. The substantial value of the rewards offered by the bug bounty program demonstrates that **TORNADO CASH** believed that bugs in these smart contracts had the potential to cause damage to **TORNADO CASH**.

4. (U) **TORNADO CASH: Trusted Setup Ceremony**

(U//~~FOUO~~) As detailed below, **TORNADO CASH** has facilitated community involvement in deployment of smart contracts through a Trusted Setup Ceremony; OFAC assesses that these ceremonies increase the profile and privacy bona fides of **TORNADO CASH**, thus increasing its appeal to users. The involvement of large numbers of participants in such a ceremony distinguishes a smart contract that has undergone the ceremony from one that has not. Trusted Setup Ceremonies also demonstrate **TORNADO CASH**'s role in serving as a coordinating mechanism for an online community of users and supporters who might otherwise be unable to organize joint action to implement a smart contract-based mixing service.

(U) According to a May 2020 blog post on the Medium website, authored by “Tornado Cash,” **TORNADO CASH** was “happy to announce that the Tornado Cash Trusted Setup Ceremony has been launched.” Tornado Cash “ask[ed the] crypto community to help make Tornado Cash fully trustless by contributing to the ceremony.” Tornado Cash explained: “We plan to end the ceremony on May 10, 2020. If there is high demand, we will keep it open for a couple more days. [Exhibit 39, pp. 1–3]

(U) According to the website of Vitalik Buterin, one of the founders of Ethereum, a trusted setup ceremony is a procedure that is done once to generate a piece of data that must then be used every time some cryptographic protocol is run. Generating this data requires some secret information; the “trust” comes from the fact that some person or some group of people has to generate these secrets, use them to generate the data, and then publish the data and forget the secrets. But once the data is generated, and the secrets are forgotten, no further participation from the creators of the ceremony is required. [Exhibit 55, p. 1]

(U//~~FOUO~~) According to the website of **TORNADO CASH**, accessed via the Wayback Machine's August 5, 2022 archive, the Tornado Cash Trusted Setup Ceremony had a searchable database of participants. OFAC queried this database [REDACTED] for Tornado Cash founders Storm, Semenov, and Pertsev and identified that each was named in the database, indicating that they were participants in the Trusted Setup Ceremony. [Exhibit 71, pp. 1–3] Based on this information, OFAC assesses that the founders of **TORNADO CASH** contributed to the Trusted Setup Ceremony.

C. (U) *The Tornado Cash Mixing Service*

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

(U) According to an August 12, 2022 press release from the Netherlands Fiscal Information and Investigation Service (FIOD), the Financial Advanced Cyber Team (FACT) of the FIOD suspects that **TORNADO CASH** has been used to conceal large-scale criminal money flows, including from (online) thefts of cryptocurrencies (so-called crypto hacks and scams). These included funds stolen through hacks by a group believed to be associated with North Korea. Investigations showed that at least one billion dollars' worth of cryptocurrencies of criminal origin passed through the mixer. [Exhibit 72, p. 1] The sections below describe how **TORNADO CASH**'s mixing service operates, and demonstrate the ways in which **TORNADO CASH** has taken concrete steps to render its services more effective at anonymizing transactions for its users, including through cultivating a large user-base, creating a network of relayers, and engaging in a yearlong anonymity mining program that rewarded users for staking assets in its smart contracts.

1. (U) *The Tornado Cash Mixing Service: How It Works*

(U) **TORNADO CASH** utilizes an array of DAO approved and implemented smart contracts to provide customers with an array of options on multiple blockchains to mix their virtual currencies. The mixing gives customers the ability to obfuscate their transactions — regardless of the source of funds, illicit or otherwise — on the blockchain of their choice. Below demonstrates how **TORNADO CASH** works to accomplish the goal of this obfuscation.

(U) According to the website of **TORNADO CASH**, accessed through the Wayback Machine's August 5, 2022 archive, "Tornado Cash improves transaction privacy by breaking the on-chain link between source and destination addresses. It uses a smart contract that accepts ETH and other tokens deposits from one address and enables their withdrawal from a different address. To maximize privacy, several steps are recommended, such as the use of a relayer for gas payments to withdraw funds from an address with no pre-existing balance." [Exhibit 120, p. 1]

(U) According to the website of **TORNADO CASH**, accessed through the Wayback Machine's August 5, 2022 archive, since its inception in 2019, **TORNADO CASH** "has been offering diversified fixed amount pools for six tokens (ETH, DAI,⁹⁸ cDAI,⁹⁹ USDC,¹⁰⁰ USDT¹⁰¹ & WBTC¹⁰²) handled by the Ethereum blockchain. Since June 2021, in addition to the Ethereum

⁹⁸ (U) According to the website of Binance, DAI is on the ERC-20 Network. [Exhibit 92, p. 2]

⁹⁹ (U) According to the website of Coinbase, Compound Dai is an algorithmic, autonomous interest protocol created for developers to unlock a range of open finance applications. The Compound is described as a protocol on the Ethereum blockchain that builds asset bundles based on the supply and demand of assets, which are pools of assets with algorithmically derived yield rates. Suppliers (and borrowers) of assets interact directly with the protocol to earn (and pay) variable rates without negotiating maturities, rates, or collateral with peers or counterparties. [Exhibit 93, p. 1]

¹⁰⁰ (U) According to the website of Binance, USDC is USD Coin and is on the ERC-20 Network. [Exhibit 92, p. 2]

¹⁰¹ (U) According to a May 16, 2022 Forbes article, Tether moves across blockchains like many other digital currencies. There are Tether tokens available on various blockchains, such as the original one with Omni on the Bitcoin platform as well as Liquid, in addition to ETH and TRON (TRX), among others. [Exhibit 124, p. 4]

¹⁰² (U) According to a May 17, 2022 Decrypt article, WBTC stands for Wrapped Bitcoin, simply an ERC-20 token that represents Bitcoin—one WBTC equals one BTC. A BTC can be converted into a WBTC and vice-versa. Being an ERC-20 token makes the transfer of WBTC faster than normal Bitcoin, but the key advantage of WBTC is its integration into the world of Ethereum wallets, DApps, and smart contracts. [Exhibit 125, p. 2]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE DECISIONAL AND DELIBERATIVE DRAFT~~

blockchain, Tornado Cash smart contracts have also been deployed on other side-chains¹⁰³ and blockchains. These deployments enabled the tool to either support new tokens or benefit from Layer-2 advantages, such as faster and cheaper transactions. As of today, Tornado Cash is operating on:

- Ethereum Blockchain: ETH (Ethereum), DAI (Dai), cDAI (Compound Dai), USDC (USD Coin),
- USDT (Tether) & WBTC (Wrapped Bitcoin),
- Binance Smart Chain:¹⁰⁴ BNB (Binance Coin),
- Polygon Network:¹⁰⁵ MATIC (Polygon),
- Gnosis Chain (former xDAI Chain): xDAI (xDai),
- Avalanche Mainnet:¹⁰⁶ AVAX (Avalanche),
- Optimism, as a Layer-2 for ETH (Ethereum), and
- Arbitrum One, as a Layer-2 ETH (Ethereum).” [Exhibit 120, p. 2]

(U) According to the website of **TORNADO CASH**, accessed through the Wayback Machine’s August 5, 2022 archive, “all pools mentioned above can be accessed on tornadocash.eth.link. They operate under the principle of fixed-amount deposits and withdrawals. It means that each token has two to four different pools, allowing transactions of only two to four different fixed amounts (e.g., ETH has four different pools, one for each of these amounts: 0.1, 1, 10 & 100 ETH).” [Exhibit 120, p. 3]

(U) According to the website of **TORNADO CASH**, accessed through the Wayback Machine’s August 5, 2022 archive, “with the release of Tornado Cash Nova (beta version) in December 2021, an upgraded pool with unique new features has been added to the protocol. Users are no longer constrained by fixed-amount transactions. With the addition of Tornado Cash Nova, they can benefit from the use of an arbitrary amount pool and shielded transfers. Tornado Cash Nova operates on the Gnosis Chain (former xDai Chain) as a Layer2 to optimize speed and cost. It allows deposits and withdrawals of completely customized amounts in ETH. This pool also enables shielded transactions where users can transfer the custody of their token while remaining in the pool.” [Exhibit 120, p. 3]

(U) According to the website of **TORNADO CASH**, accessed through the Wayback Machine’s August 5, 2022 archive, “codes behind Tornado.Cash functioning are fully open-sourced. Working as a DAO, Tornado.Cash governance and mining smart contracts are deployed by its

¹⁰³ (U) According to a March 7, 2022 CoinDesk article, a sidechain is a separate blockchain network that connects to another blockchain — called a parent blockchain or mainnet — via a two-way peg. [Exhibit 123, p. 3]

¹⁰⁴ (U) According to an April 22, 2021 CoinMarket Cap article, Binance Smart Chain is a new platform that aims to lower transaction costs and provide a space to create DApps and other DeFi. [Exhibit 126, p. 3] According to the “About” page of its website, [REDACTED] CoinMarket Cap is the world’s most-referenced price-tracking website for cryptoassets in the rapidly growing cryptocurrency space. [Exhibit 127, p. 1]

¹⁰⁵ (U) According to a February 22, 2022 Investopedia article, [REDACTED] Polygon is a cryptocurrency, with a symbol MATIC, and also a technology platform that enables blockchain networks to connection and scale. [Exhibit 129, p. 1]

¹⁰⁶ (U) According to a September 21, 2020 post on Medium, Avalanche is an open-source platform for launching decentralized finance applications and enterprise blockchain deployments in one interoperable, highly scalable ecosystem. [Exhibit 131, p. 4]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE DECISIONAL AND DELIBERATIVE DRAFT~~

community. The protocol also functions with zk-SNARK, which enables zero-knowledge proofs allowing users to demonstrate possession of information without needing to reveal it. The use of this technology is based on open-source research made by Zcash team with the help of the Ethereum community. To set up zk-SNARK initial keys, Tornado.Cash was launched in May 2020 & accounts for 1,114 contributions. This significant number of contributors makes it impossible to compromise the protocol by faking zero-knowledge proofs.” [Exhibit 120, p. 4]

(U) According to the website of **TORNADO CASH**, its UI is “hosted on IPFS (InterPlanetary File System) by the community, minimizing risks of data deletion. Indeed, the interface will work as long as at least one user is hosting it.” [Exhibit 120, p. 4]

(U) According to the website of **TORNADO CASH**, “behind the Tornado.cash front-end sits a number of Circom circuits, which enable the fundamental privacy guarantees that Tornado.cash users enjoy. These circuits implement the Zero Knowledge protocol that Tornado.cash’s smart contracts interface with to prove claims about a user’s deposit, such as that it is valid, that it has not already been withdrawn, and in the context of Anonymity Mining, the number of blocks that exist between a note’s deposit transaction and its withdrawal. Tornado.cash is best understood as having two separate major components. The core deposit circuit is what most users interact with, proving that a user has created a commitment representing the deposit of some corresponding asset denomination, that they have not yet withdrawn that asset, and that they know the secret that they supplied when generating the initial commitment. The anonymity mining circuits form the basis for the Anonymity Mining program, which incentivizes users to leave their deposits in the contract for longer periods of time, so as to ensure that the Tornado.cash deposit pools maintain a large number of active deposits (thus increasing k-anonymity¹⁰⁷ for other users).” [Exhibit 132, pp. 1, 3–4]

2. (U) *The Tornado Cash Mixing Service: How the Tornado Cash Smart Contracts Enable Mixing*

(U) As will be described below, smart contracts, including those deployed by **TORNADO CASH**, are programs running on the Ethereum blockchain. However, as noted by Coin Center, the smart contracts simply execute “deposit” and “withdrawal” operations. In and of themselves, these operations do not create a mixing service that effectively anonymizes transactions; **TORNADO CASH** also relies on a critical mass of users concurrently depositing and withdrawing transactions to obfuscate links between deposit and withdrawal addresses. As described by **TORNADO CASH** in its January 3, 2020 Medium post, user anonymity depends on the total amount of deposits made to a given smart contract as well as the behavior of other users.

¹⁰⁷ (U) According to an April 14, 2021 article by Immuta, the concept of k-anonymity was introduced into information security and privacy back in 1998. It’s built on the idea that by combining sets of data with similar attributes, identifying information about any one of the individuals contributing to that data can be obscured. k-Anonymization is often referred to as the power of “hiding in the crowd.” Individuals’ data is pooled in a larger group, meaning information in the group could correspond to any single member, thus masking the identity of the individual or individuals in question. [Exhibit 197, p. 2]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

(U) According to the August 25, 2022, post on the website of Coin Center, “Tornado Cash pools are smart contracts that enable users to transact privately on Ethereum. When prompted by a user, pools will automatically¹⁰⁸ carry out one of two supported operations: “deposit” or “withdraw.” Together, these operations allow a user to deposit tokens from one address and later withdraw those same tokens¹⁰⁹ to a different address. Crucially, even though these deposit and withdrawal events occur publicly on Ethereum’s transparent ledger, any public link between the deposit and withdrawal addresses is severed. The user can withdraw and use their funds without fear of exposing their entire financial history to third parties. A key principle of Tornado Cash pools is that a user’s privacy is derived in large part from the simultaneous usage of the pool by many other users. If the pool had only a single user, it wouldn’t matter that the link between the user’s deposit and withdrawal addresses was severed: simple inference would make it obvious where the withdrawn tokens came from. Instead, pools are used by many users simultaneously. Think of it like a bank’s safe deposit box room. Anyone can go and store valuables in a locked box in that room, and, assuming the locks are good, only the person with the key can ever get those valuables back. Security aside, however, this may or may not be privacy enhancing. If only one person is ever seen going into and out of the room, then we know any valuables in that room are theirs. If, on the other hand, many people frequently go into and out of the room, then we have no way of knowing who controls which valuables in which boxes.” [Exhibit 62, pp. 6–7]

(U) According to a January 3, 2020 Medium post by “Tornado Cash,” “although external observers cannot prove which withdrawal comes from which deposit, they can make an educated guess about it. For example:

- If a deposit and a withdrawal are right next to each other, it is very likely that they belong to the same person. We recommend waiting until at least a few deposits are made after yours before withdrawing the note.
- If there is a batch of deposits from one address, and then a batch of the same size of withdrawals to a single address, they are very likely connected. If you need to make multiple withdrawals, try to spread them out and withdraw to addresses not linked with each other.
- Wait until some time has passed after your deposit. Even if there are multiple deposits after yours, they all might be made by the same person that is trying to spam deposits and make users falsely believe that there is large anonymity set when in fact it is lower (also known as a Sybil attack). We recommend waiting at least 24 hours to make sure that

¹⁰⁸ (U//FOUO) Although Coin Center describes this process as “automatic,” OFAC assesses that this description is a simplification: as with other transactions on the Ethereum blockchain, the user must broadcast a request for the transaction to be executed on the Ethereum Virtual Machine, and a validator must select the transaction, execute it, and propagate the resulting state change to the rest of the network. This process is described in greater detail in *Section IV.A.2 (Virtual Currencies: Ethereum)* above.

¹⁰⁹ (U//FOUO) OFAC assesses that Coin Center describes users as withdrawing the “same tokens” based on the fact that **TORNADO CASH** provides a non-custodial mixing service. However, this is incorrect in a crucial respect. As detailed in Exhibit 189, tokens on the Ethereum blockchain are represented as account balances assigned to addresses. Consequently, any deposit to a smart contract deployed by **TORNADO CASH** on the Ethereum blockchain is effected by simply updating the aggregate balance of funds associated with that smart contract. Although the user retains custody of their funds in the sense that they alone have the authority to withdraw or transfer the value they deposited, their funds are commingled with assets deposited by other users of the mixing service provided by **TORNADO CASH**.”

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

there were deposits made by multiple people during that time. Check the instance statistics when using it.

- It may also be possible that making deposits or withdrawals only during waking hours of the time zone you are in can reduce your anonymity. A simple way to avoid this problem is to try your best to spread out your deposits and withdrawals as evenly across the 24 hours of each day.
- The anonymity set reflected in Tornado Cash statistics is a total amount of deposits made to a given instance. In practice, it can be lower due to various off-chain factors that are hard to formalize. For example, someone might make a Twitter post about their private transaction — it effectively means that it can be excluded from the anonymity set. Similarly in all other cases when a user deanonymizes himself, his deposit is not contributing any real anonymity. As such, it is in your interest, as well as the interest of all Tornado Cash users, to not publicize the amount that you deposit or the dates and times at which you do so (especially for withdrawals).
- In general, try to avoid any correlations that may suggest that your deposits and withdrawals are linked. A good rule of thumb is to mingle with the crowd.”
[Exhibit 60, p. 2]

(U) According to an August 10, 2022 CoinDesk article, “Tornado Cash was important not just because it worked (in theory) but because it was trusted, keys burned,” Gabagool¹¹⁰ told CoinDesk. Gabagool is referring to the destruction of the cryptographic keys needed to kick-start privacy-protecting applications, including messaging tools like PGP or blockchains like Monero. This procedure, sometimes called “key shredding,” ensures that no one has access to the cryptographic keys needed to decrypt anonymized messages or transactions. Because it typically happens at the early stages of a project, sometimes before there are any users, you often simply have to have faith that this was done and that there are no “backdoors” for bypassing the encryption. Thus, just because an alternate Tornado Cash may be running the same code does not mean you can trust it. This would be all the more complicated considering there will likely be many Tornado Cashes that spring up, causing some market confusion. Further, because Tornado Cash is operated by tumbling transactions, the liquidity of the program had a direct bearing on whether it could successfully scramble¹¹¹ the blockchain. If there were multiple Tornado Cashes, and no one could agree which was the “safe” one to use, they would all be less effective. Or in Gabagool’s words, it is likely people will redeploy the code, “but it’s not a true solve.” [Exhibit 57, pp. 4–5]

¹¹⁰ (U) According to an August 15, 2022 article on the website of The Crypto Times, Twitter handle Gabagool.eth’s owner is a coder by profession who has also earned online popularity as an on-chain investigator exposing scams and frauds. On August 4, 2022, the trading and liquidity platform Velodrome Finance recovered \$350,000 stolen in a hack from a team member. The team member was identified using the alias Gabagool. Gabagool affirmed the act and owned up to it. He revealed that Velodrome had committed the mistake of giving its private key to five team members, including him. After losing money during the crypto bear market, Gabagool withdrew \$350,000 in various cryptos which he converted to Ether and sent to Tornado Cash to recover his personal loss.
[Exhibit 56, p. 2]

¹¹¹ (U) This exhibit is discussing Tornado Cash’s tumbling (also known as mixing) services, OFAC assesses that to “Scramble the blockchain” means the process of obfuscating transactions between users of mixing services to make it difficult to trace funds from sender to receiver.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

(U//~~FOUO~~) Based on the information presented in Exhibits 57, 60, and 62, OFAC assesses that **TORNADO CASH** provides mixing services to its users not only by facilitating transactions through its smart contracts, but also by cultivating a broad user base that facilitates the anonymity of Tornado Cash transactions. Therefore, OFAC assesses that that **TORNADO CASH** provided mixing services to LAZARUS GROUP* by providing effective mixing services that allowed LAZARUS GROUP* to obfuscate its transactions. *Section V (BASES FOR DETERMINATIONS)* below further describes this activity by LAZARUS GROUP*.

3. (U) *The Tornado Cash Mixing Service: Anonymity Mining*

(U) As described in detail below, “anonymity mining” was a year-long promotion by **TORNADO CASH** which rewarded users with TORN tokens based on the amount of time they left their deposits in the **TORNADO CASH** smart contract pools.

(U) According to the website of **TORNADO CASH**, accessed through the Wayback Machine’s August 5, 2022 archive, until December 2021, the protocol included an anonymity mining system for some of these tokens, allowing its users to earn a governance token (TORN). Users were able to ultimately earn TORN on the Blockchain network by depositing in the ETH, DAI, cDAI & WBTC pools. [Exhibit 120, p. 3]

(U) According to the website of **TORNADO CASH**, accessed through the Wayback Machine’s June 17, 2022 archive, “anonymity mining is an incentive to increase the level of privacy in any coin-joining or coin-mixing protocols by rewarding participants anonymity points (AP) dependent on how long they hedge their assets in a pool. The Tornado Cash anonymity mining program began on December 18, 2020 and ended on December 18, 2021. Individuals deposited to any one of the anonymity pools that were supported (ETH, WBTC, DAI or cDAI) and were rewarded a fixed amount of AP per block, over the period their deposit remained in the pool. These points could then be exchanged for TORN once claimed. One of the community members created the resource of a mining spreadsheet that helped calculate APYs for each pool and each denomination set within, through estimating the fees required to claim a reward. The Tornado Cash website highly recommended to view this resource and plan one’s course of action before expecting to earn yield, and recommended that users always plan when deciding to mine any of the anonymity sets, to be aware that the AP/TORN rate is dependent on supply and demand, therefore, the more people that claim [AP/TORN] the higher the rate becomes, and the less people that claim the lower it becomes.” [Exhibit 138, pp. 1, 7]

4. (U) *The Tornado Cash Mixing Service: The Relay Network*

(U//~~FOUO~~) As described in detail below, a network of relayers provides a supplemental anonymizing service for Tornado Cash users withdrawing funds from Tornado Cash pools. In essence, users can pay a third-party (a “relayer”) to withdraw funds from the pool on their behalf. **TORNADO CASH** provides this service by maintaining a registry of available relayers, which is deployed to a smart contract. The relayer network also enables the collection of fees from Tornado Cash users, who pay a portion of their withdrawal transaction to the relayer. In turn, the relayers must pay **TORNADO CASH** in TORN to be listed in the relayer registry. As with the other components of **TORNADO CASH**, relayers rely on the coordination, governance, and

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

structure of the broader **TORNADO CASH** entity for their ability to function as relayers. Therefore, while an individual relayer is arguably an independent operator, OFAC assesses that the ability of Tornado Cash users to execute relayer-facilitated transactions is a functionality provided by the **TORNADO CASH** entity.

(U//~~FOUO~~) According to data from Dune,¹¹² out of a total of 145,448 withdrawal transactions from **TORNADO CASH**, 121,702¹¹³ used relayers and 23,746 were withdrawn to wallets. [Exhibit 8, p. 1]

a. (U) *The Relayer Network: How Relayers Work*

(U) According to an August 25, 2022 Coin Center article, “relayers” are independent operators that provide an optional service for Tornado Cash users. By default, when users prompt the Tornado Cash pool contracts for withdrawal, the withdrawal account needs to already have Ether to pay the Ethereum network to process the smart contract’s operations. However, sending Ether to the withdrawal account prior to withdrawal might create a link between the user’s deposit and withdrawal accounts. Relayers allow users to process withdrawals without needing to pre-fund their withdrawal accounts, which helps users maintain privacy when withdrawing. Users select a relayer from a public Relayer Registry. The user then uses their withdrawal account to sign a transaction authorizing the relayer-assisted withdrawal. The user sends this transaction to their selected relayer, who processes the withdrawal on their behalf, earning a fee in the process. According to the Coin Center article, even though they process withdrawals on behalf of users, relayers “never have custody¹¹⁴ over users’ tokens; the smart contract ensures that withdrawn tokens are only ever sent to the user’s withdrawal account.” [Exhibit 62, pp 15–16]

(U) According to the website of **TORNADO CASH**, accessed through the Wayback Machine’s June 9, 2022 archive, “relayers form an essential and necessary part of the Tornado Cash ecosystem. Their use guarantees privacy as they solve the infamous “fee payment dilemma”: how to pay fees for token withdrawals from a pool while maintaining anonymity? Therefore, relayers act as third parties and manage the entire withdrawal. They pay for transaction fees by deducting them directly from the transferred amount. They also charge an additional fee for their services.” [Exhibit 139, p. 1]

(U) According to the website of **TORNADO CASH**, accessed through the Wayback Machine’s June 9, 2022 archive, “a relayer is chosen by the user interface using the following formula:

- The list of all registered relayers is retrieved from the Relayer Registry smart contract.

¹¹² (U) According to its website, “Dune is a powerful tool for blockchain research. Dune gives you all the tools to query, extract, and visualize vast amounts of data from the blockchain. Dune is unlocking the power of public blockchain data by making it accessible to everyone.” [Exhibit 79, p. 1]

¹¹³ (U//~~FOUO~~) This figure represents 83.67 percent of the total withdrawal transactions.

¹¹⁴ (U) In this context, “custody” has a technical meaning with respect to cryptocurrency. According to the website of CoinDesk, cryptocurrency is essentially a bearer asset, as the person who holds the private keys to a wallet effectively controls (owns) the coins inside. Custodial wallets are wallet services offered by a centralized business such as a cryptocurrency exchange. When a user outsources wallet custody to a business, they are essentially outsourcing their private keys to that institution. Non-custodial wallets do not require the outsourcing of trust to an institution, so no institution can refuse to complete transactions. [Exhibit 97, pp. 2–3]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

- For each relayer, calculate a score based on its staked TORN and its fee. The higher the stake, the higher the score is; the higher the fee, the lower the score is. For Ethereum mainnet, the formula used to calculate the score is $\text{stake} * [1 - 25 * (\text{fee} - 0.33)^2]$; for sidechains, the formula is $\text{stake} * [1 - 11.89 * (\text{fee} - 0.01)^2]$.
- Then randomly pick a relayer, weighted by its calculated score.” [Exhibit 139, pp. 1–2]

(U) The website of **TORNADO CASH**, accessed through the Wayback Machine’s June 9, 2022 archive, provides instructions to “anyone [wishing to] become a relayer for the protocol in 6 simple steps through a Relayer Registry User Interface.

1. Warning: Understand & Accept Potential Risks. Before you commit to sharing part of your journey with Tornado Cash users as a relayer, you need to understand & accept all potential risks of being a relayer for the protocol.
2. The first concrete step is to run the Tornado Cash Relayer software for Ethereum Mainnet on your computer. All steps are outlined in the protocol’s github. To complete this task successfully, you will have to carefully follow these instructions. Once completed, you will need to insert your url in the input box. It is strongly recommended that you use your own RPC nodes.¹¹⁵
3. Set up Ethereum Name Service (ENS)¹¹⁶ Subdomain. The next steps entail: creating an ENS domain for your relayer; setting up its mainnet subdomain; adding a TXT record with the Relayer URL to the mainnet subdomain. You also have the option to add subdomains with their corresponding TXT records to support chains other than Ethereum. Sidechains relayers use a different version of the Relayer software. Tornado Cash Nova uses its own version of the software.
4. Workers are the addresses that will allow your relayer to send ZK-proofs to users. By default, the first worker is the ENS domain owner’s address.
5. With the implementation of a decentralized relayer registry, a staking condition has been introduced as a requirement to become listed on Tornado Cash UI. Keep in mind staking TORN is now necessary to be added to the recommended list of relayers. The minimum staked amount is currently set by Tornado Cash governance at 300 TORN. This threshold can be changed by Tornado Cash governance at any time. When a relayer is used in the Tornado Cash pool, a small amount of TORN is automatically collected from this staked balance by the Staking Reward contract. This element is essential to keep in mind as relayers will need to keep enough TORN locked (~40 TORN in April 2022) to be able to pay back the transaction fee to the staking contract. The collected fees are subsequently distributed among DAO members with locked TORN tokens. TORN are usually locked to participate in on-chain governance (submitting & voting on proposals). Your staked TORN amount is not claimable, and it is non-refundable.
6. Summary: Final Verification & Registration.” [Exhibit 139, pp. 1–6]

¹¹⁵ (U) According to the website of Coinbase, a Remote Procedure Call or RPC node is a type of computer server that allows users to read data on the blockchain and send transactions to different networks. [Exhibit 140, p. 1]

¹¹⁶ (U) According to a May 12, 2022 BeinCrypto Article, ENS refers to Ethereum Name Service, and is a naming protocol that allows humans to use easy-to-remember domain names for their cryptocurrency addresses. The protocol then translates it to a machine-readable address. This process has many similarities to the DNS system we use for the internet. Furthermore, it empowers users with a tool that can unify their online presence and help them step into the realm of web3. [Exhibit 184, p. 1]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE DECISIONAL AND DELIBERATIVE DRAFT~~

(U) According to **TORNADO CASH**'s website, accessed through the Wayback Machine's February 18, 2022 archive, "relayers are used to withdraw to an account with no ETH balance. The relayer sends a withdrawal transaction and takes a part of the deposit as compensation (though the protocol itself does not collect any fees). The relayer cannot change any withdrawal data including recipient address. The Tornado Cash initial developers do not control or play any role in relaying transactions; the relay network is independent and run by the community." [Exhibit 64, p. 7]

(U//~~FOUO~~) Although relayers independently set their fees, and the relayer fees are paid directly to the relayers, **TORNADO CASH** separately collects a per-transaction fee in TORN from relayers. This mechanism is explained in further detail in the remainder of this section and in the next section.

(U//~~FOUO~~) According to an August 25, 2022 Coin Center article, the relayer registry is the smart contract 0x58E8dCC13BE9780fC42E8723D8EaD4CF46943dF2 ("0x58E8d"). According to Coin Center, the relayer registry can be updated pending a Tornado Cash community vote. [Exhibit 62, p. 24] Because the smart contract can be updated by the Tornado Cash community,¹¹⁷ OFAC assesses that **TORNADO CASH** has the ability to thereby manage the relayer registry.

(U//~~FOUO~~) According to Etherscan, smart contract 0x58E8d has a total of 722 transactions. The most recent transaction to smart contract 0x58E8d occurred on September 20, 2022 and executed the function "stake to relayer." [Exhibit 96, p. 1] Based on the substantial number of transactions, OFAC assesses that Tornado Cash relayers regularly stake to the relayer smart contract or otherwise interact with the relayer smart contract.

(U) According to the website of **TORNADO CASH**, which was archived by the Internet Archive on June 9, 2022, following the execution of Tornado Cash tenth governance proposal, anyone can become a relayer for Tornado Cash users. The only condition to be included on the Tornado Cash UI is to lock a min[imum] of 300 TORN.¹¹⁸ To remain listed, it is needed to keep enough TORN locked (~ 40 TORN in April 2022) to be able to pay back the transaction fee to the staking contract. Since the implementation of the Relayer Registry proposal, the protocol collects a fee directly from the relayer's staked balance through the "Staking Reward" contract for each withdrawal. This fee percentage may vary from one pool to another and is also subject to change through on-chain governance. Currently¹¹⁹ it is fixed at 0.3 percent. Some pools remain without fees, either because the instance is too small to assign a fee (0.1 ETH, 100

¹¹⁷ (U) OFAC assesses the term "community" as used in this and other exhibits includes, but is not limited to, holders of TORN and developers of Tornado Cash.

¹¹⁸ (U) According to a note in the exhibit, this minimum stake can be changed by a governance vote at any time. [Exhibit 139, p. 1]

¹¹⁹ (U//~~FOUO~~) OFAC assesses that this information was current as of the date it was archived, June 9, 2022.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

DAI/USDT, 1000 DAI/USDT), or because there is not enough liquidity on Uni[swap] v3¹²⁰ (all cDAI instances). [Exhibit 139, p. 1]

D. (U) ***TORNADO CASH's Property and Interests in Property***^{121, 122}

1. (U) **TORNADO CASH's Interest in the TORNADO CASH Smart Contracts**

(U//~~FOUO~~) According to the website of Ethereum, creating a smart contract has a cost because you are using network storage. [Exhibit 58, p. 2] Because creating a contract on the Ethereum blockchain has a cost, OFAC assesses that any given contract has a nonzero monetary value. Because creating a smart contract requires initiating a transaction and paying a fee, OFAC assesses that users create smart contracts because they regard the functionality of the smart contract as having value. Accordingly, OFAC assesses that **TORNADO CASH** regarded smart contracts created on its behalf as having value; that **TORNADO CASH** has derived value from smart contracts created on its behalf; and that therefore **TORNADO CASH** has an interest in such smart contracts.

(U//~~FOUO~~) Based on information presented in this memorandum, OFAC assesses that **TORNADO CASH** has an interest in the smart contracts created on its behalf because use, popularity, and success of the smart contracts increases the economic value of **TORNADO CASH** and of the TORN tokens, including those held by **TORNADO CASH** itself as well as those issued by the DAO to individual DAO members. The DAO issued TORN tokens to early

¹²⁰ (U//~~FOUO~~) According to Uniswap's website, Uniswap v1 was launched in November 2018 as a proof of concept for automated market makers (AMMs), a type of exchange where anyone can pool assets into shared market making strategies. In May 2020, Uniswap v2 introduced new features and optimizations. As of March 23, 2021, Uniswap v3 was introduced. [Exhibit 141, p. 1] OFAC assesses v3 refers to version three of Uniswap.

¹²¹ (U) The relevant OFAC regulations define "interest," when used with respect to property (e.g., "an interest in property"), as "an interest of any nature whatsoever, direct or indirect." 31 C.F.R. §§ 510.313, 578.309. "Property" and "property interest" are defined as follows:

The terms *property* and *property interest* include money, checks, drafts, bullion, bank deposits, savings accounts, debts, indebtedness, obligations, notes, guarantees, debentures, stocks, bonds, coupons, any other financial instruments, bankers acceptances, mortgages, pledges, liens or other rights in the nature of security, warehouse receipts, bills of lading, trust receipts, bills of sale, any other evidences of title, ownership, or indebtedness, letters of credit and any documents relating to any rights or obligations thereunder, powers of attorney, goods, wares, merchandise, chattels, stocks on hand, ships, goods on ships, real estate mortgages, deeds of trust, vendors' sales agreements, land contracts, leaseholds, ground rents, real estate and any other interest therein, options, negotiable instruments, trade acceptances, royalties, book accounts, accounts payable, judgments, patents, trademarks or copyrights, insurance policies, safe deposit boxes and their contents, annuities, pooling agreements, services of any nature whatsoever, contracts of any nature whatsoever, and any other property, real, personal, or mixed, tangible or intangible, or interest or interests therein, present, future, or contingent.

31 C.F.R. §§ 510.323, 578.314.

¹²² (U) Similar to the physical address of a real estate property that is owned by a blocked person, the digital currency addresses of Tornado Cash smart contracts may refer to interests in property of **TORNADO CASH** and also serve as identifiers associated with **TORNADO CASH**.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE DECISIONAL AND DELIBERATIVE DRAFT~~

backers and users, including the original developers, who can profit by selling tokens on virtual currency exchanges, and changes in the price of TORN tokens appear to correlate with expectations surrounding the success of the smart contracts. TORN owners and the DAO are in this way similar to stockholders, who have an interest in the enterprise, and may benefit from the success of **TORNADO CASH**. Accordingly, the more users that submit virtual currency to the smart contracts to be mixed, the larger the pool becomes, and the more effectively the virtual currency may be mixed, thereby increasing the value of **TORNADO CASH** and of TORN tokens.

(U//~~FOUO~~) According to a May 1, 2020 blog post on the website of Medium, authored by "Tornado Cash," "Tornado Cash is happy to announce that the Tornado Cash Trusted Setup Ceremony has been launched, we ask crypto community to help make Tornado Cash fully trustless by contributing to the ceremony. We plan to end the ceremony on May 10, 2020. If there is high demand, we will keep it open for a couple more days. Tornado Cash utilizes zk-SNARK technology to provide anonymity for withdrawals. The zk-SNARK requires a trusted setup which is a special procedure that generates the prover and verifier keys. In order to make sure that it is done in a secure way, no one is able to fake proofs or steal user funds it should be done in a decentralized way. To fake zk proofs, an attacker must compromise every single participant of the ceremony. Therefore, the probability of it goes down as the number of participants goes up. The purpose of the ceremony is to generate Verifier smart contract. After completion, our team will update all Verifiers in all instances and set the operator address to zero. At this point Tornado Cash smart contracts will become completely immutable and unstoppable." [Exhibit 39, pp. 1–3] Because organizing and coordinating these setup ceremonies would require the expenditure of time and effort, OFAC assesses that a smart contract that has undergone this setup ceremony is more valuable than one that has not. Based on **TORNADO CASH** announcing the setup ceremony and soliciting participants in it, OFAC assesses that value created through this setup ceremony was generated for the benefit of **TORNADO CASH**.

(U//~~FOUO~~) According to a December 15, 2021 post on the website of Medium, authored by "Tornado Cash," **TORNADO CASH** introduced "Tornado Cash Nova," an upgraded Tornado Cash pool¹²³ presenting unique features focused on improving user experience and expanding the protocol functionalities. This pool will allow users to deposit and withdraw arbitrary amounts of ETH. Up to now, all Tornado Cash pools had one thing in common: users could only deposit and withdraw a fixed amount of a given token within each pool. With the arrival of the Nova pool, this statement will no longer be true. An improved v3 of the Tornado Cash protocol is being currently prepared. This incoming version mainly focuses on enhancing users' experience. Some handy new features are planned to bring more flexibility and possibilities to the use of the protocol. With its customized amounts and shielded transfers, "Tornado Cash Nova" is the first step towards this new and improved version of Tornado Cash. Future plans for the protocol include the possibility of making atomic swaps¹²⁴ within a shielded pool, as well as a pool that

¹²³ (U//~~FOUO~~) Given that the "pools" described in this exhibit receive funds and facilitate obfuscation, OFAC assesses that the referenced "pools" are references to Tornado Cash smart contracts.

¹²⁴ (U) According to an August 14, 2022 Investopedia article, "Atomic Swap Definition," an atomic swap is an exchange of cryptocurrencies from separate blockchains. The swap is conducted between two entities without a

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

will be able to support ERC-20 tokens & NFT. [Exhibit 15, pp. 2, 5] OFAC assesses that these efforts by **TORNADO CASH** to advertise improvements in its mixing service in aid of maximizing its number of users, as evidenced in Exhibit 15 and throughout this memorandum, show that **TORNADO CASH** has an interest in the deployed smart contracts, including those that contain these touted improvements.

2. (U) **TORNADO CASH's Interest in the TORN Smart Contract**

(U//~~FOUO~~) As described above in *Sections IV.B.2 (TORNADO CASH: Decentralized Autonomous Organization (DAO))* and *IV.C.6 (The Tornado Cash Mixing Service: The Relayer Network)*, **TORNADO CASH** created the TORN token through a smart contract deployed on the Ethereum blockchain. OFAC assesses that **TORNADO CASH** thus controlled governance and disbursement of TORN tokens. **TORNADO CASH** structured payouts of TORN tokens so that they incentivize use of the Tornado Cash mixing service. In particular, **TORNADO CASH** airdropped TORN to users of the service. In addition, the “anonymity mining” program rewarded users with TORN based on the length of time that they held assets in Tornado Cash smart contract pools. As described above, the greater the quantity of assets held in the Tornado Cash smart contract pools, the greater the efficacy of the Tornado Cash mixing service. Therefore, by implementing the anonymity mining program, **TORNADO CASH** used its control over disbursement of TORN tokens to enhance the efficacy of the Tornado Cash mixing service, increasing the value of its service and smart contracts.

(U//~~FOUO~~) As described above, **TORNADO CASH** disbursed only a portion of the maximum total supply of 10 million TORN tokens. **TORNADO CASH** distributed a majority of TORN tokens to the custody of **TORNADO CASH** itself through several smart contracts.

(U) According to Etherscan, as of October 1, 2022, eight of the top ten addresses holding the most TORN tokens are Tornado Cash smart contract addresses. The address that holds the most TORN tokens is the Tornado Cash Governance Vesting smart contract, which holds 4,125,000 TORN tokens worth approximately \$26.3 million. The address that holds the third-most TORN tokens is the Tornado Cash Governance smart contract, which holds approximately 1,258 TORN tokens worth approximately \$8 million. [Exhibit 90, p. 1]

(U//~~FOUO~~) As described in *Section IV.B.2 (TORNADO CASH: Decentralized Autonomous Organization (DAO))*, **TORNADO CASH** has used the TORN it controlled to fund development and enhancement of the **TORNADO CASH** mixing service. It has offered to pay TORN to contributors to **TORNADO CASH** and offered bug bounties in TORN to those who identified security vulnerabilities in its smart contracts.

(U//~~FOUO~~) Based on the explanation in Exhibit 5, showing that relayers must pay a fee directly to the **TORNADO CASH** DAO, and based on the fact that TORN holders can receive a portion of these fees based on the amount of TORN they have staked, OFAC assesses that **TORNADO**

third party's involvement. The idea is to remove centralized intermediaries like regulated exchanges and give token owners total control. [Exhibit 68, p. 1]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

CASH has an interest in user transactions that are withdrawn through relayers, and in the TORN tokens used in that process.

3. (U) **TORNADO CASH's Interest in Pool and Relayer Smart Contracts**

(U//~~FOUO~~) According to the August 25, 2022 post on the website of Coin Center, "a key principle of Tornado Cash pools is that a user's privacy is derived in large part from the simultaneous usage of the pool by many other users. If the pool had only a single user, it would not matter that the link between the user's deposit and withdrawal addresses was severed: simple inference would make it obvious where the withdrawn tokens came from. Instead, pools are used by many users simultaneously. Think of it like a bank's safe deposit box room. Anyone can go and store valuables in a locked box in that room, and, assuming the locks are good, only the person with the key can ever get those valuables back. Security aside, however, this may or may not be privacy enhancing. If only one person is ever seen going into and out of the room, then we know any valuables in that room are theirs. If, on the other hand, many people frequently go into and out of the room, then we have no way of knowing who controls which valuables in which boxes." [Exhibit 62, pp. 6-7] Because the efficacy of **TORNADO CASH** as a mixer depends on a critical mass of users depositing funds to its pool smart contracts, OFAC assesses that **TORNADO CASH's** efforts to entice more and more users to deposit funds into its smart contracts is evidence of **TORNADO CASH's** interest in the funds that users have deposited into its smart contracts.

(U//~~FOUO~~) According to data from Dune, out of a total of 145,448 withdrawal transactions from Tornado Cash, 121,702 used relayers and 23,746 were withdrawn to wallets. [Exhibit 8, p. 1] Because relayers were used in the substantial majority of withdrawal transactions from **TORNADO CASH**, OFAC assesses that tokens held in the **TORNADO CASH** smart contract pools have the potential to generate fees for **TORNADO CASH** because of the fees required to use relayers. OFAC therefore assesses that **TORNADO CASH** has an interest in such funds.

(U//~~FOUO~~) According to data from Dune, in the week of August 29, 2022, relayer fees for Tornado Cash paid to Governance in U.S. dollars were \$76,135. [Exhibit 77, p. 1] Based on this information, OFAC assesses that **TORNADO CASH** was receiving fees generated through use of its pool and relayer smart contracts. These facts further evidence that **TORNADO CASH** has an interest in the pool and relayer smart contracts.

(U//~~FOUO~~) According to the "Staking" section of **TORNADO CASH's** website, with the introduction of a decentralized relayer register, a staking reward has been implemented for all holders with locked TORN in the governance contract. TORN holders can still lock their tokens into the governance contract as they used to for governance purposes. The significant difference is that they are now able to receive a portion of the fees collected by the protocol from relayers. In a nutshell, for each withdrawal through the relayer method, the chosen relayer has to pay a fee to the protocol from the staked balance (that should still be maintained above the 300 TORN threshold). Currently, this fee has been fixed at 0.3 percent by the governance and can be changed at any time through an on-chain [proposal of change and corresponding vote].

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

[Exhibit 5, p. 1] Based on the fact that the Tornado Cash Governance Contract¹²⁵ receives a fee from each withdrawal through the relayer method, OFAC assesses that **TORNADO CASH** has an interest in such withdrawals.

(U//~~FOUO~~) As described previously in *Section IV.C.6 (The Tornado Cash Mixing Service: The Relayer Network)*, becoming a relayer listed on the **TORNADO CASH** UI requires staking TORN to the Tornado Cash Governance Contract. **TORNADO CASH** collects a fee from this staked TORN each time the relayer is used to facilitate a withdrawal from the **TORNADO CASH** pool smart contracts. In return, the relayer receives a portion of the withdrawal (for example, a relayer receives ETH for withdrawals from ETH pools). As **TORNADO CASH** deducts fees from the relayer's staked TORN, the relayer must acquire and stake more TORN in order to continue acting as a relayer. Consequently, higher volume usage of the Tornado Cash mixing service, resulting in greater numbers of withdrawals via relayers, creates additional demand for TORN tokens. Therefore, based on **TORNADO CASH**'s interest in and holdings of TORN tokens, OFAC assesses that **TORNADO CASH** has an interest in its mixing service as deployed via the pool, relayer, and other smart contracts.

E. (U) *Foreign Person Property Interest Nexus*¹²⁶

1. (U) *Interest of North Korea*

(U) According to a February 9, 2021 Reuters¹²⁷ article, a preliminary United Nations (UN) inquiry into the theft of \$281 million worth of assets from a cryptocurrency exchange in September 2020 "strongly suggests" links to North Korea—with industry analysts pointing to Seychelles-based KuCoin as the victim of one of the largest reported digital currency heists. A confidential report by independent sanctions monitors to UN Security Council members said blockchain transactions related to the hack also appeared to be tied to a second hack last October when \$23 million was stolen. "Preliminary analysis, based on the attack vectors and subsequent efforts to launder the illicit proceeds, strongly suggests links to the DPRK," the monitors wrote. They accuse Pyongyang of using stolen funds to support its nuclear and ballistic missile

¹²⁵ (U) As detailed above, the Tornado Cash governance contract plays an essential role in the operation and governance of **TORNADO CASH** and of the service provided by **TORNADO CASH**.

¹²⁶ (U) Section 203 of the International Emergency Economic Powers Act ("IEEPA"), authorizes the President to:

investigate, block during the pendency of an investigation, regulate, direct and compel, nullify, void, prevent or prohibit, any acquisition, holding, withholding, use, transfer, withdrawal, transportation, importation or exportation of, or dealing in, or exercising any right, power, or privilege with respect to, or transactions involving, *any property in which any foreign country or a national thereof has any interest* by any person, or with respect to any property, subject to the jurisdiction of the United States.

50 U.S.C. § 1702(a)(1)(B) (emphasis added). Thus, OFAC may block or prohibit even domestic transactions where a foreign country or national thereof has an interest in the underlying property.

¹²⁷ (U) According to the homepage of its website, accessed on April 29, 2022, Reuters, the news and media division of Thomson Reuters, is the world largest multimedia news provider, reaching billions of people worldwide every day. Reuters provides business, financial, national, and international news to professionals via desktop terminals, the world's media organizations, industry events, and directly to consumers. [Exhibit 147, p. 16]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE DECISIONAL AND DELIBERATIVE DRAFT~~

programs to circumvent sanctions. While the report did not name the victim of the attack, digital currency exchange KuCoin reported the theft of \$281 million in bitcoin and various other tokens on September 25, 2020. [Exhibit 180, pp. 1–2]

(U) According to a February 2022 Chainalysis report, LAZARUS GROUP* first gained notoriety from its Sony Pictures and WannaCry cyberattacks, but it has since concentrated its efforts on cryptocurrency crime—a strategy that has proven immensely profitable. From 2018 on, the group has stolen and laundered massive sums of virtual currencies every year, typically in excess of \$200 million. The most successful individual hacks, one on KuCoin and another on an unnamed cryptocurrency exchange, each netted more than \$250 million alone. And according to the UN security council, the revenue generated from these hacks goes to support North Korea's WMD and ballistic missile programs. [Exhibit 178, p. 114]

(U//~~FOUO~~) According to blockchain analysis conducted by OFAC, funds stolen in the KuCoin hack were subsequently transferred to Ethereum address 0xA160cdAB225685dA1d56aa342Ad8841c3b53f291, which is attributed by Chainalysis to **TORNADO CASH**. This transfer of funds occurred between October 19, 2020 and October 21, 2020, in a series of 134 transactions of 100 ETH each. The total value of these transfers was over \$5 million. [Exhibit 181, p. 2]

(U) According to the website of Etherscan, address 0xA160cdAB225685dA1d56aa342Ad8841c3b53f291 is a Tornado Cash smart contract and was deployed by another Tornado Cash smart contract, address 0x8589427373D6D84E98730D7795D8f6f8731FDA16. [Exhibit 182, p. 1]

(U//~~FOUO~~) Based on the above information, OFAC assesses that threat actors acting on behalf of North Korea transferred funds to **TORNADO CASH** between October 19, 2020 and October 21, 2020. This attribution is strengthened by North Korean threat actors' repeated use of the service provided by **TORNADO CASH** to launder stolen funds, as described further throughout this memorandum.

(U//~~FOUO~~) As described previously in Exhibit 4, **TORNADO CASH** airdropped TORN tokens to addresses that had used its mixing service prior to December 6, 2020. Because North Korean threat actors used the service provided by **TORNADO CASH** during this timeframe, and because **TORNADO CASH** did not implement any mechanism to prevent illicit actors from benefiting from its airdrop, OFAC assesses that North Korean threat actors received TORN in **TORNADO CASH**'s airdrop, and consequently received the ability to participate in voting on changes to the service provided by **TORNADO CASH**.

(U//~~FOUO~~) As described previously in *Section IV.B.2 (TORNADO CASH: Decentralized Autonomous Organization (DAO))*, TORN is **TORNADO CASH**'s governance token. In addition, as described in *Section IV.C.6 (The Tornado Cash Mixing Service: The Relay Network)*, value generated through use of the Tornado Cash mixing service accrues to holders of TORN through distribution of fees and an increase in the value of TORN. Therefore, North Korea's ownership of TORN tokens created an interest of North Korea in **TORNADO CASH**.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

2. (U) Foreign Person Founders and Developers

(U) The below individuals have been identified as key developers of **TORNADO CASH** who likely received a portion of the 30% of available TORN tokens that were locked for a period of three years, as described in Exhibit 4:

- (U//~~FOUO~~) According to an August 19, 2022¹²⁸ CoinMarket Cap article, “Another Russian national that is in the crosshairs of the Dutch authorities is Alexey Pertsev the arrested Tornado Cash developer. [Exhibit 11, p. 2] OFAC assesses that Alexey Pertsev is a Russian national because Exhibit 11 refers to Alexey Pertsev as “another Russian national.”
- (U) According to an August 24, 2022 report by Kharon,¹²⁹ Alexey Pertsev, a resident of the Netherlands, is a founder and the CEO of PepperSec, according to personal and company profiles reviewed by Kharon. In 2017, Alexey Pertsev was an information security specialist and developer of smart contracts for DIGITAL SECURITY OOO*,¹³⁰ according to an archived version of the company’s website reviewed by Kharon. DIGITAL SECURITY OOO* is a Russian entity designated by the U.S. Treasury Department in 2018 for providing material and technological support to the FEDERAL SECURITY SERVICE* (FSB*)¹³¹, Russia’s primary security agency. Treasury alleged that, as of 2015, DIGITAL SECURITY OOO* worked on a project that would increase the offensive cyber capabilities of Russia’s intelligence services. [Exhibit 42, p. 3]
- (U//~~FOUO~~) According to Crunchbase,¹³² Roman Semenov, a co-founder of **TORNADO CASH**, is located in Moscow, Russia, and is a co-founder of the company PepperSec. [Exhibit 13, p. 1] Given the fact that Roman Semenov is located in Russia, OFAC assesses that Roman Semenov is a Russian national.

3. (U) Foreign Person TORN Token Holders

(U) According to the website of Etherscan, accessed August 19, 2022, the TORN holdings of the following addresses¹³³ attributed to foreign entities are as follows:

¹²⁸ (U//~~FOUO~~) While there is no date on this article, it states that it was updated 5 days ago, and was accessed by OFAC on August 24, 2022. Therefore, OFAC assesses the article was updated on August 19, 2022.

¹²⁹ (U) According to its website, Kharon’s risk data and software solutions are unparalleled in precision and depth, powering compliance, risk management, investigations, and analytic operations at the world’s leading institutions. [Exhibit 43, p. 2]

¹³⁰ (U) On June 11, 2018, DIGITAL SECURITY OOO* was designated by the Department of the Treasury pursuant to E.O. 13694 for providing material and technological support to the FSB*. [Exhibit 44, p. 1–2]

¹³¹ (U) On December 28, 2016, the FSB* was listed in the annex of E.O. 13694, as amended. [Exhibit 45, p. 3] On March 2, 2021, the FSB* was designated by the U.S. Department of State pursuant to E.O. 13382 for having engaged, or attempted to engage, in activities or transactions that have materially contributed to, or pose a risk of materially contributing to, the proliferation of weapons of mass destruction or their means of delivery (including missiles capable of delivering such weapons), including any efforts to manufacture, acquire, possess, develop, transport, transfer or use such items, by Russia. [Exhibit 46, p. 4]

¹³² (U) According to its website, Crunchbase allows users to search, track, and monitor companies’ customers care about using best-in-class private company data. [Exhibit 33, p. 1]

¹³³ (U) The list below contains the label for the address on the website on the website of Etherscan, rather than the address itself.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

- Binance 8¹³⁴: 1,658,151 TORN;
- OKEx: 218,635 TORN;
- Binance 14: 50,174 TORN
- Binance 15: 11,746 TORN
- Binance 16: 13,341 TORN
- 1inch: 6,069 TORN [Exhibit 10, pp. 1–2]

(U) According to an October 29, 2020 Forbes article, Binance is currently known to be Cayman Islands based, but the exchange first launched in Shanghai. Later as the Chinese government cracked down on cryptocurrency trading, the company moved its headquarters to Japan and then Malta. In May 2020 [Binance founder Changpeng Zhao] told former Forbes staffer Laura Shin that Binance's headquarters were wherever he was. His answer wasn't necessarily evasive but presented as a rally cry for blockchain's ideals of decentralized power. [Exhibit 98, p. 7]

(U) According to its website OKEx is a virtual currency exchange located in Seychelles. [Exhibit 31, p. 1]

(U) According to the Securities Exchange Commission, 1inch is registered in the British Virgin Islands. [Exhibit 32 p. 1]

(U) According to the website of Etherscan, as of October 1, 2022, an address attributed to Binance was the second-largest holder of TORN and held over 18 percent of all TORN, equivalent to approximately \$11.5 million. [Exhibit 90, p. 1]

(U) According to the website of Binance, as of October 1, 2022, TORN tokens are available for trade and were trading at \$6.37. [Exhibit 37, p. 1]

(U) According to the website of Binance, [REDACTED] Binance claims that it is "unable to provide services to U.S. users. Binance.US (BAM Trading Services) is a U.S.-regulated cryptocurrency trading platform. In approved states, U.S. customers can use Binance.US to buy and sell over 50 cryptocurrencies with low fees." [Exhibit 91, p. 1]

(U) According to the website of Binance.US, [REDACTED] Binance.US currently support 100+ digital assets. TORN was not included in this list of assets. [Exhibit 92, pp. 1, 4]

(U//~~FOUO~~) Based on the above information, OFAC assesses that user deposits of TORN held in custody by Binance are at least in substantial part the property of non-U.S., foreign persons.

V. (U) BASES FOR DETERMINATIONS

A. (U) *Designation Pursuant to E.O. 13694, as Amended*

¹³⁴ (U//~~FOUO~~) OFAC assesses that the numbering of these addresses distinguishes multiple addresses that have been attributed to the same entity.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

(U//~~FOUO~~) In March 2022, DPRK's LAZARUS GROUP* carried out a heist of the Axie Sky Mavis Ronin Network, which is the largest cyber heist to date. LAZARUS GROUP* stole over \$600 million worth of the virtual currency Ether and subsequently carried out an extensive money laundering operation. The money laundering operation was an effort to separate the source and destination of funds. **TORNADO CASH**, a provider of virtual currency mixing services, received the majority of these funds and provided its obfuscating services to LAZARUS GROUP* to make it more difficult for authorities to trace the funds from the victim to the cyber actors who carried it out.

1. (U) *Sky Mavis-Ronin Bridge Heist* (Cyber-Enabled Activity)

a. (U//~~FOUO~~) *The Sky Mavis-Ronin Bridge Heist is a cyber-enabled activity originating from, or directed by persons located, in whole or in substantial part, outside the United States that is reasonably likely to result in, or has materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that has the purpose or effect of causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain.*

(U) According to a March 30, 2022 Reuters article, hackers have stolen virtual currency worth almost \$615 million from a blockchain project linked to the popular online game Axie Infinity. Ronin, a blockchain network that lets users transfer crypto in and out of the game, said on Tuesday, March 29, 2022, that the theft happened on March 23, 2022, but was not detected until almost a week later. Ronin produces a digital wallet for storing crypto, and a "bridge" that allows users to move funds into and out of the online game. This is where crypto was stolen from. Sky Mavis is a Vietnam-based company that launched Axie Infinity in 2018.¹³⁵ [Exhibit 145, pp. 3–4]

(U) According to a March 30, 2022 *Barron's*¹³⁶ article, the *Sky Mavis-Ronin Bridge Heist* is disconcerting partly because of the size of the theft, but also because of how it transpired. Ronin is managed by just nine computer "nodes" that validate transactions in the network. Typically, it takes a majority of nodes to form a consensus on the validity of a transaction, enabling it to be recorded on the blockchain. In this case, the hackers gaining control of just five nodes did the trick. [Exhibit 146, pp. 1–2]

(U//~~FOUO~~)



¹³⁵ (U) Due to the association of Sky Mavis and Axie Infinity with this heist, OFAC will refer to it as the *Sky Mavis-Ronin Bridge Heist*, although some media reports also refer to it as the "Ronin heist."

¹³⁶ (U) According to the "About" page of its website, accessed on April 14, 2022, *Barron's* is a financial journal whose founder believed the press should be Wall Street's watchdog. [Exhibit 148, p. 4]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

137

138

139

[Exhibit 153, p. 10]

(U//FOUO)

40

[Exhibit 153, p. 11]

(U//FOUO) According to an April 14, 2022 Federal Bureau of Investigation (FBI) press statement, the FBI continues to combat malicious cyber activity including the threat posed by DPRK to the United States and its private sector partners. Through its investigation FBI was able to confirm LAZARUS GROUP* cyber actors associated with DPRK, are responsible for the theft of \$620 million ETH reported on March 29, 2022. The FBI in coordination with Treasury and other U.S. government partners, will continue to expose and combat DPRK's use of illicit activities, including cybercrime and virtual currency theft to generate revenue for the regime. [Exhibit 159, p. 1] This press statement is referring to the *Sky Mavis-Ronin Bridge Heist*, which was reported on March 29, 2022, given the approximate \$620 million value and occurrence on March 29, as described in Exhibit 145 and Exhibit 146 and attributed to the DPRK by the FBI in Exhibit 159 [REDACTED] in addition to OFAC and FBI's close coordination on this matter. Accordingly, OFAC assesses that the *Sky Mavis-Ronin Bridge Heist* is a cyber-enabled activity originating from, or directed by persons located, in whole or in substantial part, outside the United States.

b. (U//FOUO) *The Sky Mavis-Ronin Bridge Heist is a cyber-enabled activity originating from, or directed by persons located, in whole or in substantial part, outside the United States that is reasonably likely to result in, or has materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that has the purpose or effect of causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain.*

(U//FOUO) According to the April 14, 2022 FBI press statement, the FBI continues to combat malicious cyber activity including the threat posed by DPRK to the United States and our private

¹³⁷ (U) According to a July 31, 2020 CoinDesk Article, a spear-phishing attack is a targeted attempt to steal information such as account details or financial information from a particular individual. [Exhibit 150, p. 3]

¹³⁸ (U) According to a February 25, 2022 Medium article, validators store a copy of the blockchain and must perform certain functions to keep the system secure. [Exhibit 154, p. 1]

¹³⁹ (U) According to an October 14, 2020 Medium article, a third-party validator is a validator-as-a-service that have dedicated infrastructure and personnel to solely run validators for other people. [Exhibit 156, p. 1]

¹⁴⁰ (U) According to a January 6, 2021 CoinDesk article, RAT refers to a Remote Access Tool. [Exhibit 158, p. 3]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

sector partners. Through its investigation FBI was able to confirm LAZARUS GROUP* cyber actors associated with DPRK are responsible for the theft of \$620 million ETH reported on March 29, 2022. The FBI in coordination with Treasury and other U.S. government partners, will continue to expose and combat DPRK's use of illicit activities, including cybercrime and virtual currency theft to generate revenue for the regime. [Exhibit 159, p. 1] This press statement is referring to the *Sky Mavis-Ronin Bridge Heist*, which was reported on March 29, 2022, given the approximate \$620 million value and occurrence on March 29, as described in Exhibit 145 and Exhibit 146 and attributed to DPRK by the FBI in Exhibit 159 [REDACTED]

(U) According to an April 14, 2020 DPRK Cyber Threat Advisory jointly authored by the State Department, Treasury Department, Department of Homeland Security, and the FBI, DPRK's malicious cyber activities threaten the United States and the broader international community and, in particular, pose a significant threat to the international financial system. Under pressure of robust U.S. and UN sanctions, DPRK has increasingly relied on illicit activities, including cybercrime, to generate revenue for its WMD and ballistic missile programs. In particular, the United States is deeply concerned about DPRK's malicious cyber activities. DPRK has the capability to conduct disruptive and harmful cyber activity that is wholly inconsistent with the growing international consensus on what constitutes responsible State behavior in cyberspace. [Exhibit 174, p. 1]

(U) According to Annex I in the April 14, 2020 joint cyber threat advisory, the Office of the Director of National Intelligence's Annual Worldwide Threat Assessments of the U.S. Intelligence Community (IC) noted in 2019 that DPRK poses a significant cyber threat to financial institutions, remains a cyber-espionage threat, and retains the ability to conduct disruptive cyber-attacks. DPRK continues to use cyber capabilities to steal more than \$1.1 billion from financial institutions across the world—including a successful cyber heist of an estimated \$81 million from Bangladesh Bank. [Exhibit 174, p. 9]

(U//~~FOUO~~) Given the facts that DPRK executed the *Sky Mavis-Ronin Bridge Heist*, as demonstrated in Exhibit 159, and DPRK uses funds derived from malicious cyber activities to fund its WMD and ballistic missiles programs, as described in Exhibit 174, OFAC assesses that the *Sky Mavis-Ronin Bridge Heist* is reasonably likely to result in, or has materially contributed to, a significant threat to the national security of the United States.

c. (U//~~FOUO~~) *The Sky Mavis-Ronin Bridge Heist is a cyber-enabled activity originating from, or directed by persons located, in whole or in substantial part, outside the United States that is reasonably likely to result in, or has materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that has the purpose or effect of causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain.*

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

(U//FOUO) [REDACTED]

¹⁴¹

[Exhibit 153, p. 10]

(U) According to a March 29, 2022 Bloomberg article, on March 23, 2022 hackers stole about \$600 million from a blockchain network connected to the popular Axie Infinity online game in one of the biggest crypto attacks to date. Computers known as nodes operated by Axie Infinity maker Sky Mavis and the Axie DAO that support a so-called bridge software that lets people convert tokens into ones that can be used on another network were attacked, with the hacker draining what's known as the *Sky Mavis-Ronin Bridge Heist* of 173,600 ETH and \$25.5 million USDC tokens in two transactions. [Exhibit 171, pp. 1–2]

(U) According to an August 30, 2019 U.N. Report from the Panel of Experts, the panel investigated the widespread and increasingly sophisticated use of cyber means by DPRK to illegally force the transfer of funds from financial institutions and virtual currency exchanges, launder stolen proceeds, and generate income in evasion of financial sanctions. In particular, large-scale attacks against virtual currency exchanges allow DPRK to generate income in ways that are harder to trace and subject to less government oversight and regulations than the traditional banking sector. DPRK cyber actors raise money for their country's WMD program with total proceeds to date estimated at up to \$2 billion. [Exhibit 168, p. 4]

(U//FOUO) OFAC assesses that the *Sky Mavis-Ronin Bridge Heist* had the purpose or effect of causing a significant misappropriation of funds for commercial or competitive advantage, namely, the advantage of an injection of an estimated \$620 million in difficult-to-trace funds into DPRK's WMD program—funds that would not have been available to DPRK but for the illicit cyber-enabled activity.

2. (U) **TORNADO CASH** (Entity)

(U//FOUO) *TORNADO CASH* has materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of the *Sky Mavis-Ronin Bridge Heist*, an activity described in section 1(a)(ii) of E.O. 13694, as amended.

(U) According to a March 11, 2022, Finance Brokerage¹⁴² article, “one of the founders of Tornado Cash, one of the most popular obfuscation services for crypto transactions, said it does not have to comply with sanctions imposed after Russia attacked Ukraine. The protocol is designed to preserve privacy by disconnecting the sender and receiver addresses in transactions over the Ethereum blockchain. The project is based on smart contracts which means ready-made

¹⁴¹ (U) [REDACTED]

¹⁴² (U) According to the “About Us” page of its website, [REDACTED] Finance Brokerage is a comprehensive financial and market news platform that is accessed by thousands of people all around the world. [Exhibit 162, p. 2]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

software programs rather than individuals making decisions. It also does not offer to host services, nor does it have a central host for its website. Individuals can access Tornado Cash using the Ethereum Name Service. It [Ethereum Name Service] is a credential free distributed naming system that the co-founder says helps make monitoring users impossible.” [Exhibit 161, p. 1]

(U) According to an April 4, 2022 Bloomberg article, “a hacker moved some of the roughly \$600 million in cryptocurrency stolen from the Axie Infinity play-to-earn gaming platform to a service that helps users mask transactions. About 2,000 ETH tokens, valued at around \$7 million, that were lifted from Axie Infinity’s Ronin software bridge¹⁴³ last month [March 2022] were moved Monday [April 4] to Tornado Cash, blockchain data shows. Tornado Cash is designed to preserve privacy on the Ethereum blockchain. Its technology breaks the link between the sender and receiver’s addresses on transactions sent to the Ethereum blockchain. The protocol has been used in the past by hackers who took \$34 million from Crypto.com. “Tracking funds after any mixer, including Tornado Cash, is a probabilistic method and we cannot be 100 percent certain,” blockchain analysis firm Merkle Science wrote in an email response. The main ETH address used by the hackers who attacked Axie Infinity’s Ronin blockchain sent 2,001 ETH to another ETH address earlier Monday [April 4]. The second ETH address then sent 2,000 ETH in batches of 100 ETH each to Tornado Cash, blockchain data shows. The transactions were confirmed by blockchain data firm Nansen.” [Exhibit 163, p. 1]

(U//FOUO)

144

145

¹⁴³ (U//FOUO) OFAC assesses that the theft of roughly \$600 million in cryptocurrency from “Axie Infinity’s Ronin Software bridge” is referring to the *Sky Mavis-Ronin Bridge Heist*, given the approximate \$620 million value and occurrence on March 29, 2022, as described in Exhibit 145 and Exhibit 146.

¹⁴⁴ (U//FOUO)

¹⁴⁵ (U)

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE DECISIONAL AND DELIBERATIVE DRAFT~~

[Exhibit 153, pp. 10–11]

(U//~~FOUO~~) Given that the funds of *Sky Mavis-Ronin Bridge Heist* were processed through the service provided by **TORNADO CASH** [REDACTED], OFAC assesses that **TORNADO CASH** has provided material support to the *Sky Mavis-Ronin Bridge Heist*, namely, by providing transaction obfuscation services meant to separate the trail of the source of the stolen funds to the cyber-enabled malicious actors.

(U//~~FOUO~~) Additional information to support OFAC's designation of **TORNADO CASH** is available in the classified addendum to this memorandum.

B. (U) Designation Pursuant to E.O. 13722

(U) TORNADO CASH (Entity)

(U//~~FOUO~~) *TORNADO CASH has materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, the Government of North Korea. (E.O. 13722)*

(U) According to a September 13, 2019 U.S. Treasury Department Press release, "Today, OFAC announced sanctions targeting three North Korean state-sponsored malicious cyber groups responsible for North Korea's malicious cyber activity on critical infrastructure. Today's actions identify North Korean hacking groups commonly known within the global cyber security private industry as "Lazarus Group," "Bluenoroff," and "Andariel" as agencies, instrumentalities, or controlled entities of the Government of North Korea pursuant to E.O. 13722, based on their relationship to the RECONNAISSANCE GENERAL BUREAU* (RGB*). LAZARUS GROUP*, Bluenoroff, and Andariel are controlled by the U.S.- and UN-designated RGB*, which is North Korea's primary intelligence bureau." [Exhibit 113, pp. 1–2]

(U) According to a March 30, 2022 Reuters article, hackers have stolen virtual currency worth almost \$615 million from a blockchain project linked to the popular online game Axie Infinity. Ronin, a blockchain network that lets users transfer crypto in and out of the game, said on Tuesday, March 29, 2022, that the theft happened on March 23, 2022, but was not detected until almost a week later. Ronin produces a digital wallet for storing crypto, and a "bridge" that allows users to move funds into and out of the online game. This is where crypto was stolen from. Sky Mavis is a Vietnam-based company that launched Axie Infinity in 2018. [Exhibit 145, pp. 3–4]

(U) According to an April 14, 2022 FBI press statement, "The FBI continues to combat malicious cyber activity including the threat posed by DPRK to the United States and our private sector partners. Through our investigation we were able to confirm LAZARUS GROUP* cyber actors associated with DPRK, are responsible for the theft of \$620 million ETH reported on March 29, 2022. The FBI in coordination with Treasury and other U.S. government partners, will continue to expose and combat DPRK's use of illicit activities, including cybercrime and virtual currency theft to generate revenue for the regime." [Exhibit 159, p. 1] This press

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE DECISIONAL AND DELIBERATIVE DRAFT~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

statement is referring to the same stolen virtual currency crime described in Exhibit 145, which was reported on March 29, 2022, given the approximate \$620 million value and occurrence on March 29, as described in Exhibit 145.

(U) According to an April 18, 2022, Department of Homeland Security, Cybersecurity Infrastructure and Security Agency (CISA) advisory, the FBI, and Treasury are issuing this joint Cybersecurity Advisory (CSA) to highlight the cyber threat associated with cryptocurrency thefts and tactics used by a North Korean state-sponsored advanced persistent threat (APT) group since at least 2020. This group is commonly tracked by the cybersecurity industry as LAZARUS GROUP*, APT38, Bluenoroff, and Stardust Chollima. [Exhibit 167, p. 1]

(U) According to an August 30, 2019 U.N. Report from the Panel of Experts, the panel investigated the widespread and increasingly sophisticated use of cyber means by DPRK to illegally force the transfer of funds from financial institutions and virtual currency exchanges, launder stolen proceeds, and generate income in evasion of financial sanctions. In particular, large-scale attacks against virtual currency exchanges allow DPRK to generate income in ways that are harder to trace and subject to less government oversight and regulations than the traditional banking sector. DPRK cyber actors raise money for their country's WMD program with total proceeds to date estimated at up to \$2 billion. [Exhibit 168, p. 4]

(U) According to an April 14, 2020 DPRK Cyber Threat Advisory jointly authored by the State Department, Treasury Department, Department of Homeland Security, and the FBI, DPRK's malicious cyber activities threaten the United States and the broader international community and, in particular, pose a significant threat to the international financial system. Under pressure of robust U.S. and U.N. sanctions, DPRK has increasingly relied on illicit activities, including cybercrime, to generate revenue for its WMD and ballistic missile programs. In particular, the United States is deeply concerned about DPRK's malicious cyber activities. DPRK has the capability to conduct disruptive and harmful cyber activity that is wholly inconsistent with the growing international consensus on what constitutes responsible State behavior in cyberspace. [Exhibit 174, p. 1]

(U) According to Annex I of the April 14, 2020 joint cyber threat advisory, the Office of the Director of National Intelligence's Annual Worldwide Threat Assessments of the U.S. IC noted in 2019 that DPRK poses a significant cyber threat to financial institutions, remains a cyber-espionage threat, and retains the ability to conduct disruptive cyber-attacks. DPRK continues to use cyber capabilities to steal more than \$1.1 billion from financial institutions across the world—including a successful cyber heist of an estimated \$81 million from Bangladesh Bank. [Exhibit 174, p. 9]

(U) According to an April 13, 2022 FBI Letterhead Memorandum (LHM) to OFAC, an FBI investigation into the malicious cyber activity of the DPRK dubbed in open source as LAZARUS GROUP* has revealed that ETH address 0x098B716B8Aaf21512996dC57EB0615e2383E2f96

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

("E2f96")¹⁴⁶ is a hacker-controlled digital currency address used by the LAZARUS GROUP*. [Exhibit 169, p. 1]

(U//FOUO) [REDACTED]

[Exhibit 153, pp. 10–11]

(U) According to a June 29, 2022 Elliptic,¹⁴⁷ blogpost, "on the morning of June 24, 2022 over \$100 million in crypto assets was stolen from Horizon Bridge—a service that allows assets to be transferred between the Harmony blockchain and other blockchains. Our analysis of the hack and the subsequent laundering of the stolen crypto assets also indicates that it is consistent with activities of the LAZARUS GROUP*. Although no single factor proves the involvement of LAZARUS GROUP*, in combination they suggest the group's involvement:

- The LAZARUS GROUP* has perpetrated several large cryptocurrency thefts totaling over \$2 billion, and has recently turned its attention to DeFi services such as cross-chain bridges. For example, the group is believed to be behind the \$540 million hack of Ronin Bridge.
- The theft was perpetrated by compromising the cryptographic keys of a multi-signature wallet—likely through a social engineering attack on Harmony team members. Such techniques have frequently been used by the LAZARUS GROUP*.
- The stolen crypto assets included ETH, USDT, WBTC and BNB. The thief immediately used Uniswap — a decentralized exchange (DEX) — to convert the Ethereum-based assets into a total of 85,837 ETH. This is a common laundering technique used to avoid seizure of stolen assets.
- The regularity of the deposits into Tornado Cash over extended periods of time suggests that an automated process is being used. We have observed very similar programmatic laundering of funds stolen from the Ronin Bridge, which has been attributed to LAZARUS GROUP*, as well as a number of other attacks linked to the group." [Exhibit 225, pp. 1–3]

(U//FOUO) According to blockchain analysis conducted by OFAC [REDACTED]¹⁴⁸ **TORNADO CASH** received stolen funds from at least one additional LAZARUS GROUP* virtual currency heist beyond the *Sky Mavis-Ronin Bridge Heist*:

- U.S. company Harmony Heist, aka Harmony Protocol Exploit, June 23, 2022:
 - On June 23, 2022, virtual currency address 0x58F4BACcb411ACef70A5f6DD174Af7854fc48Fa9 sent

¹⁴⁶ (U) "2f96" was added to the LAZARUS GROUP* SDN List entry as an identifying feature on April 14, 2022. [Exhibit 170, p. 1]

¹⁴⁷ (U) According to its website, Elliptic provides blockchain analytics for financial crime compliance.

[Exhibit 24, p. 1]

¹⁴⁸ (U//FOUO) [REDACTED]

[Exhibit 27, p. 4]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

0x0d043128146654C7683Fbf30ac98D7B2285DeD00 a total of 41,562 ETH in eight transactions.

- Between June 23–24, 2022, virtual currency address 0x9E91ae672E7f7330Fc6B9bAb9C259BD94Cd08715 sent 0x0d043128146654C7683Fbf30ac98D7B2285DeD00 a total of 31,207 ETH in 10 transactions.
- On June 23, 2022, virtual currency address 0xF50B2077d40830b2AC77f9147c65DD5E8D5b8557 sent 0x0d043128146654C7683Fbf30ac98D7B2285DeD00 a total of 0.99 ETH in two transactions.
- On June 27, 2022, 0x0d043128146654C7683Fbf30ac98D7B2285DeD00 sent 0x1Ec6F83b55C3F4CeFc630442716872BA15f16430 a total of 18,036.3 ETH in one transaction.
- On June 27, 2022 0x1Ec6F83b55C3F4CeFc630442716872BA15f1 6430 sent:
 - 6,009 ETH to 0x1Ec6F83b55C3F4CeFc630442716872BA15f16430;
 - 6,012 ETH to 0x432A9Cb4353bed67EC5351734d4a44C0826847Ae, and;
 - 6,012 ETH to 0x4507Aclbdf4Ae5E61ffceC3A9AEDA312E2505970
- On June 27, 2022, 0x1Ec6F83b55C3F4CeFc630442716872BA15f1 6430 sent 6,000 ETH to **TORNADO CASH**.
- On June 27, 2022, 0x432A9Cb4353bed67EC5351734d4a44C0826847Ae sent 6,000 ETH to **TORNADO CASH**.
- On June 27, 2022, 0x4507Aclbdf4Ae5E61ffceC3A9AEDA312E2505970 sent 6,000 ETH to **TORNADO CASH**. [Exhibit 164, pp. 2–3]

(U//~~FOUO~~) As described by Exhibit 145 and Exhibit 159, LAZARUS GROUP* carried out a March 2022 cyber heist of \$620 million worth of virtual currency. As described by Exhibit 113, LAZARUS GROUP* is an agency, instrumentality, or entity controlled by the GONK*. As described in Exhibit 164 and Exhibit 225, DPRK carried out the Harmony heist and **TORNADO CASH** facilitated the laundering of funds derived from the heist. As described by Exhibit 168 and Exhibit 174, the GONK* has used laundered proceeds of virtual currency thefts to support its WMD and ballistic missile programs. [REDACTED] **TORNADO CASH** facilitated the laundering of proceeds from the March 2022 cyber heist. Therefore, OFAC assesses that **TORNADO CASH** has provided material support to the GONK*.

(U//~~FOUO~~) Additional information to support OFAC's designation of **TORNADO CASH** is available in the classified addendum to this memorandum.

VI. (U) **ADDITIONAL INFORMATION**

(U//~~FOUO~~) According to blockchain analysis conducted by OFAC [REDACTED] **TORNADO CASH** also laundered funds derived from the U.S. company Nomad Heist in August 2022 this heist has not been publicly attributed to any specific actor:

- On August 2, 2022, 0xC9943f94142D81790eCf8EEE2C879d47730cf599 sent:
 - 2,580 ETH to 0x8d5DEe51D984809D83Fe7E474755A15686121124 in two transactions.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

- 1,003 ETH to 0xbC09E7aD2adbla2D2aFC403514287AdD5fC10B9F in two transactions.
- 1,205 ETH to 0x7a98B3F0d6e2907594Da0D97529C5cc678dFa308 in two transactions.
- On August 2, 2022, 0x8d5DEe51D984809D83Fe7E474755A15686121124 sent 2,500 ETH to **TORNADO CASH** in 25 transactions.
- On August 2, 2022, 0xbC09E7aD2adbla2D2aFC403514287AdD5fC10B9F sent 1,000 ETH to **TORNADO CASH** in 10 transactions.
- On August 2, 2022, 0x7a98B3F0d6e2907594Da0D97529C5cc678dFa308 sent 1,200 ETH to **TORNADO CASH** in 12 transactions. [Exhibit 164, p. 2–3]

(U//~~FOUO~~) According to data [REDACTED], on August 2, 2019, **TORNADO CASH** received transactions worth a combined total of approximately \$7 billion between its founding and August 3, 2022. [Exhibit 164, p. 3]

(U) OFAC conducted blockchain analysis of three heists that laundered funds through **TORNADO CASH**:

- Sky Mavis Ronin Bridge Heist: \$455,594,329.
- Nomad Bridge Heist: approximately \$7.8 million
- Harmony Heist: approximately: \$96 million [Exhibit 207, pp. 2–5]

(U) According to an April 15, 2022 CoinDesk article, “Tornado Cash said Friday [April 15, 2022] “it is using a tool developed by compliance firm Chainalysis to block crypto wallets sanctioned by OFAC. However, the blockade only applies to the user-facing DApp, not the underlying smart contract,” one of the protocol’s founders later tweeted. [Tornado Cash], which claims to defend people’s financial privacy, has often been used to obfuscate the trail of crypto obtained through hacks. The protocol’s founder has previously said it is “technically impossible” to enforce sanctions on decentralized protocols like Tornado Cash. “There’s not much we can do,” he said in a March 2022 interview.” [Exhibit 166, pp. 2–3]

(U) According to the website of **TORNADO CASH**, accessed via the Wayback Machine, the Tornado Cash Trusted Setup Ceremony had a searchable database of participants. OFAC queried this database [REDACTED] for **TORNADO CASH** founders Roman Storm, Roman Semenov, and Alexey Pertsev, and identified that each was named in the database, indicating that they had been participants in the Trusted Setup Ceremony. [Exhibit 71, pp. 1–3]

(U//~~FOUO~~) As described below, because cryptocurrencies use a ledger that can be viewed by anyone, users of cryptocurrencies may have concerns regarding their privacy that are distinct from those of users of traditional financial services. Cryptocurrency mixing services, such as those offered by **TORNADO CASH**, purport to be among the efforts to respond to such privacy concerns.

(U) According to a 2019 Thomson Reuters Practical Law Practice Note, “some blockchain technology features can help mitigate or cater to privacy concerns, such as using encryption and verifying data integrity. However, blockchain technology’s distributed peer-to-peer network architecture often places it at odds with the traditional notion of centralized controller-based data

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

processing. This disconnect can make it difficult to reconcile current data protection laws with blockchain's other core elements, such as the lack of centralized control, immutability, and perpetual data storage." [Exhibit 104, p. 3]

(U) According to the same 2019 Practical Law Practice Practice Note, "blockchains, including many public blockchains that support popular cryptocurrencies, tout anonymity or at least some level of privacy by using public-private key pair encryption. These asymmetric encryption systems leverage the mathematical relationship between the public and private keys in a particular pair; record public keys on the blockchain implementation; do not typically record public key owner data or other similar personal information; and leave users to retain and protect their own private keys." [Exhibit 104, p. 3]

(U) According to the same 2019 Practical Law Practice Practice Note, "some blockchain enthusiasts claim that using public-private key encryption preserves anonymity and privacy. This is a relatively simplistic view of personal information because methods exist for linking individuals to public keys by analyzing blockchain transactions and other publicly available data. Some businesses offer services to identify individuals using their public keys, blockchain transactions, and other available data. Better practice treats public keys as tokenizations of personal information from a privacy perspective instead of anonymized data, because they correspond to an individual and reidentification becomes possible in some circumstances. Reidentification risks and related concerns have led some blockchains, including privacy-focused cryptocurrencies, to try to reduce the risk of identifying individual participants by implementing various mitigation strategies to protect transaction and other data and introducing alternative cryptographic approaches." [Exhibit 104, p. 4]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE DECISIONAL AND DELIBERATIVE DRAFT~~

EXHIBITS LIST

- Exhibit 1: (U) Website of CoinDesk, "What is Tokenomics and Why is it Important?" accessed October 1, 2022, available at: <https://www.coindesk.com/learn/what-is-tokenomics-and-why-is-it-important/>. (U).
- Exhibit 2: (U) Executive Order 13551 of August 30, 2010, "Blocking Property of Certain Persons With Respect to North Korea," Vol. 75 No. 169. (U).
- Exhibit 3: (U) [REDACTED] (U//LES).
- Exhibit 4: (U) Website of Tornado Cash, "Torn," archived version from June 17, 2022, accessed via The Wayback Machine, available at: <https://web.archive.org/web/20220617060943/https://docs.tornado.cash/general/torn> (U).
- Exhibit 5: (U) Website of Tornado Cash, "Staking," archived version from April 20, 2022, accessed via The Wayback Machine, available at: <https://web.archive.org/web/20220420103225/https://docs.tornado.cash/general/staking> (U).
- Exhibit 6: (U) Website of CoinDesk, "Tornado Cash Co-Founder Says the Mixer Protocol is Unstoppable," January 25, 2022, accessed August 22, 2022, available at: www.coindesk.com/tech/2022/01/25/tornado-cash-co-founder-says-the-mixer-protocol-is-unstoppable/ (U).
- Exhibit 7: (U) Website of Decrypt.co, "Tornado Cash Ethereum Token Down 50% After Sanctions," August 12, 2022, accessed August 22, 2022, available at: <https://decrypt.co/107382/tornado-cash-ethereum-token-down-50-after-sanctions> (U).
- Exhibit 8: (U) Website of Dune, "Tornado Cash," [REDACTED] available at: dune.com/poma/tornado-cash_1 (U).
- Exhibit 9: (U) Website of Etherscan, "Address 0x4e7B3769921C8DFBdb3d1B4c73558db079A180c7, [REDACTED] available at: <https://etherscan.io/address/0x4e7b3769921c8dfbdb3d1b4c73558db079a180c7> (U).
- Exhibit 10: (U) Website of Etherscan, "TORN Token," [REDACTED] available at: <https://etherscan.io/token/0x77777feddddfc19ff86db637967013e6c6a116c#balances> (U).

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

- Exhibit 11: (U) Website of CoinMarket Cap, "Russian Ransomware Attacker Extradited to U.S. from Netherlands, Tornado Cash Dev Still Isolated," August 19, 2022, [REDACTED] available at: <https://coinmarketcap.com/alexandria/article/russian-ransomware-attacker-extradited-to-us-from-netherlands-tornado-cash-dev-still-isolated> (U).
- Exhibit 12: (U) Website of BTC Geek, "Write for Us," [REDACTED] available at: <https://btcgeek.com/write-for-us>. (U).
- Exhibit 13: (U) Website of Crunchbase, "Roman Semenov," [REDACTED] available at: www.crunchbase.com/person/roman-semenov (U).
- Exhibit 14: (U) Website of Open Zeppelin, "OpenZeppelin Contracts," [REDACTED] available at: <https://openzeppelin-contracts/Proxy.sol> (U).
- Exhibit 15: (U) Website of Medium, "Tornado Cash Introduces Arbitrary Amounts & Shielded Transfers," December 15, 2021, available at: <https://tornado-cash.medium.com/tornado-cash-introduces-arbitrary-amounts-shielded-transfers-8df92d93c37c>. (U).
- Exhibit 16: (U) Website of TechTarget, "User Interface," [REDACTED] available at: www.techtarget.com/searcharchitecture/definition/user-interface-UI (U).
- Exhibit 17: (U) Website of SPDX, "Overview," [REDACTED] available at: <https://spdx.dev/about/> (U).
- Exhibit 18: (U) Website of Cointelegraph, "Tornado Cash community fund multisignature wallet disbands amid sanctions," August 15, 2022, available at: <https://cointelegraph.com/news/tornado-cash-community-fund-multi-signature-wallet-disbands-amid-sanctions> (U).
- Exhibit 19: (U) Website of ImmuneFi, "About," [REDACTED] available at: <https://immune.fi/about/>. (U).
- Exhibit 20: (U) Website of Internet Archive, "About," [REDACTED] available at: <https://archive.org/about/> (U).
- Exhibit 21: (U) Website of Investopedia, "What Crypto Users Need to Know: The ERC20 Standard," updated August 24, 2021 [REDACTED] available at: www.investopedia.com/tech/why-crypto-users-need-know-about-erc20-token-standard/ (U).
- Exhibit 22: (U) Website of Cointelegraph, "What is a crypto airdrop, and how does it work" July 14, 2022, accessed August 18, 2022 available at:

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE DECISIONAL AND DELIBERATIVE DRAFT~~

<https://cointelegraph.com/news/what-is-a-crypto-airdrop-and-how-does-it-work> (U).

- Exhibit 23: (U) Website of Cointelegraph, "About," accessed April 1, 2022, available at: <https://cointelegraph.com/about/> (U).
- Exhibit 24: (U) Website of the Elliptic, "Our Story," [REDACTED] available at: <https://www.elliptic.co/our-story>. (U).
- Exhibit 25: (U) Website of Cointelegraph, "Understanding Staking Pools: The Pros and cons of staking cryptocurrency," May 9, 2022, accessed August 25, 2022, available at: <https://cointelegraph.com/explained/understanding-staking-pools-the-pros-and-cons-of-staking-cryptocurrency> (U).
- Exhibit 26: (U) Website of Chainalysis, "About Us," [REDACTED] available at: www.chainalysis.com/company/ (U).
- Exhibit 27: (U//FOUO) [REDACTED]
(U//FOUO) [REDACTED]
- Exhibit 28: (U) Website of SPDX MIT, "MIT License," [REDACTED] available at: <https://spdx.org/licenses/MIT.html> (U).
- Exhibit 29: (U) Website of Etherscan, "About Etherscan," [REDACTED] available at: <https://etherscan.io/aboutus> (U).
- Exhibit 30: (U) Website of Etherscan, "Transaction Details 0xab," [REDACTED] available at: <https://etherscan.io/tx/0xab822174f2b6177867d53eeea05ed7e80965b9b412f42f5a55674fe900399019> (U).
- Exhibit 31: (U) Website of OKX, "Contact Us," [REDACTED] available at: www.okx.com/contactu-us.html (U).
- Exhibit 32: (U) Securities Exchange Commission, "1inch LTD," accessed August 25, 2022, available at: <https://sec.report/CIK/0001830516> (U).
- Exhibit 33: (U) Website of Crunchbase, "About Crunchbase," July 28, 2017, available at: www.about.crunchbase.com/about-us/ (U).
- Exhibit 34: (U) Website of Bitcoin.com, "Tornado Cash Governance Token TORN Shudders More than 57% Since the US government Ban," August 13, 2022, [REDACTED] available at: news.bitcoin.com/tornado-cash-governance-token-torn-shudders-more-than-57-since-the-us-government-ban/ (U).

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

- Exhibit 35: (U) Website of Decrypt, "What is 1inch Exchange? Beginners Guide," June 23, 2021, accessed October 7, 2022, available at: <https://decrypt.co/resources/1inch-dex-aggregator-decentralized-exchanges> (U).
- Exhibit 36: (U) Website of Etherscan, "Address 0x5efda50f22d34f262c29268506C5Fa42cB56A1Ce," [REDACTED] available at: <https://etherscan.io/address/0x5efda50f22d34f262c29268506c5fa42cb56a1ce> (U).
- Exhibit 37: (U) Website of Binance, "TORN," [REDACTED] available at: www.binance.com/en/trade/TORN_BUSD?_from=markets&theme=dark&type=spot (U).
- Exhibit 38: (U) Website of Github, "Gnosis Chain / media-kit," [REDACTED] available at: <https://github.com/gnosischain/media-kit>. (U).
- Exhibit 39: (U) Website of Medium, "Tornado.cash Trusted Setup Ceremony," May 1, 2020, available at: <https://tornado-cash.medium.com/tornado-cash-trusted-setup-ceremony-b846e1e00be1> (U).
- Exhibit 40: (U) Website of Altcoin Buzz, "About Altcoin Buzz," [REDACTED] 2022, available at: <https://www.altcoinbuzz.io/about-altcoin-buzz/>. (U).
- Exhibit 41: (U) Website of Medium, "What is Medium?," accessed April 29, 2022, available at: www.medium.com/about?autoplay=1 (U).
- Exhibit 42: (U) Website of Kharon, "Developer of Sanctioned Crypto Mixer Arrested, Was Employed by Company Linked to Russia's FSB," August 24, 2022, available at: <https://brief.kharon.com/updates/ceo-of-sanctioned-crypto-mixer-arrested-was-employed-by-company-linked-to-russia-s-fsb/> (U).
- Exhibit 43: (U) Website of Kharon, "About Kharon," [REDACTED] available at: www.kharon.com/#kharon-company (U).
- Exhibit 44: (U) Website of the Department of the Treasury, "Treasury Sanctions Russian Federal Security Service Enablers," June 11, 2018, available at: <https://home.treasury.gov/news/press-releases/sm0410> (U).
- Exhibit 45: (U) Executive Order 13757 of December 28, 2016, "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities," 82 Fed. Reg. 1 (January 3, 2017) (U).
- Exhibit 46: (U) U.S. Department of State, Press Release, "U.S. Sanctions and Other Measures Imposed on Russia in Response to Russia's Use of Chemical

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

Weapons,” March 2, 2021, available at: www.state.gov/u-s-sanctions-and-other-measures-imposed-on-russia-in-response-to-russias-use-of-chemical-weapons/ (U).

- Exhibit 47: (U) Website of Investopedia, “Hot Wallet,” [REDACTED] available at: investopedia.com/terms/h/hot-wallet.asp. (U).
- Exhibit 48: (U) Website of GitHub, “Tornado Repositories,” [REDACTED] available at: <https://github.com/tornado-repositories> (U).
- Exhibit 49: (U) Website of CoinTelegraph, “DeFi Staking a Beginners Guide to proof-of-Stake Coins,” accessed October 24, 2022, available at: <https://cointelegraph.com/defi-101/defi-staking-a-beginners-guide-to-proof-of-stake-pos-coins#:~:text=Staking%20pools%20allow%20people%20to,the%20amount%20on%20their%20holdings.> (U).
- Exhibit 50: (U) Website of Ethereum, “Introduction to Ethereum Governance,” August 29, 2022, [REDACTED] available at: <https://ethereum.org/en/governance/> (U).
- Exhibit 51: (U) Website of Blockchain Council, “What is Dai?,” May 13, 2022, [REDACTED] available at: <https://www.blockchain-council.org/dao/what-is-dai/>. (U).
- Exhibit 52: Website of DeCrypt, “What is Compound?” April 20, 2020, accessed October 6, 2022, available at: <https://decrypt.co/resources/compound-defi-ethereum-explained-guide-how-to>. (U).
- Exhibit 53: (U) [REDACTED]
(U//FOUO).
- Exhibit 54: (U) Website of the Department of the Treasury, Press Releases, “Treasury Takes Robust Actions to Counter Ransomware,” September 21, 2021, available at: <https://home.treasury.gov/news/press-releases/jy0364>. (U).
- Exhibit 55: (U) Website of Vitalik, “How do Trusted Setups Work?” March 14, 2022, [REDACTED] available at: vitalik.ca/general/2022/03/14/trusted.html (U).
- Exhibit 56: (U) Website of Cryptotimes, “Velodrome Regains \$350k Stolen by its Developer Gabagool,” August 15, 2022, [REDACTED] available <https://www.cryptotimes.io/velodrome-regains-350k-stolen-by-its-developer-gabagool/> (U).

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

- Exhibit 57: (U) Website of Coindesk, "Cloning Tornado Cash Would Be Easy, but Risky," accessed September 16, 2022, available at: www.coindesk.com/tech/2022/08/10/cloning-tornado-cash-would-be-easy-but-risky/ (U).
- Exhibit 58: (U) Website of Ethereum, "Ethereum Accounts," [REDACTED] available at: <https://ethereum.org/en/developers/docs/accounts/> (U).
- Exhibit 59: (U) Chainalysis, "Dissecting the DAO: Web3 Ownership is Surprisingly Concentrated," [REDACTED] available at: <https://blog.chainalysis.com/reports/web3-daos-2022/> (U).
- Exhibit 60: (U) Website of Medium, "How to Stay Anonymous with Tornado.cash and similar solutions," [REDACTED] available at: <https://tornado-cash.medium.com/how-to-stay-anonymous-with-tornado-cash-and-similar-solutions-efdecdbd7d37> (U).
- Exhibit 61: (U) Website of Medium, "Tornado.Cash Governance Proposal," archived version from December 18, 2020 accessed via The Wayback Machine, available at: <https://web.archive.org/web/20220808144451/https://tornado-cash.medium.com/tornado-cash-governance-proposal-a55c5c7d0703#bf59> (U).
- Exhibit 62: (U) Website of Coin Center, "How does Tornado Cash work?" August 25, 2022, [REDACTED] available at: www.coincenter.org/education/advanced-topics/how-does-tornado-cash-work/ (U).
- Exhibit 63: (U) Website of Chainalysis, "Crypto Mixers and AML Compliance," August 23, 2022, [REDACTED] available at: <https://blog.chainalysis.com/reports/crypto-mixers/> (U).
- Exhibit 64: (U) Website of Tornado Cash, "How Tornado Cash Works," archived version from February 18, 2022, accessed via The Wayback Machine [REDACTED] available at: <https://web.archive.org/web/20220218214742/https://tornado.cash/> (U).
- Exhibit 65: (U) Website of the Department of the Treasury, Press Releases, "Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange," November 8, 2021, available at: <https://home.treasury.gov/news/press-releases/jy0471>
- Exhibit 66: (U) Website of Investopedia, "Application Programming Interface (API)," [REDACTED] available at: investopedia.com/terms/a/application-programming-interface.asp (U).

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

- Exhibit 67: (U) Website of Snapshot, "Home-Snapshot," [REDACTED] available at: <https://docs.snapshot.org> (U).
- Exhibit 68: (U) Website of Investopedia, "Atomic Swap Definition," August 14, 2022, [REDACTED] available at: <https://www.investopedia.com/terms/a/atomic-swaps.asp#:~:text=An%20atomic%20swap%20is%20an,give%20token%20owners%20total%20control.> (U).
- Exhibit 69: (U) Website of Medium, "What Are Cliffs And Vesting, And Why Do They Matter?" December 9, 2021, accessed September 13, 2022, available at: <https://medium.com/@playSIPHER/what-are-cliffs-and-vesting-and-why-do-they-matter-8c21eec37c99> (U).
- Exhibit 70: (U) Website of Medium, "What's Up Tornado – Some Digging on Tornado Cash Decision Making," September 6, 2021, archived version from August 8, 2022, accessed via The Wayback Machine on September 9, 2022, available at: <https://web.archive.org/web/20220808144523/https://wutornado.medium.com/whats-up-tornado-some-digging-on-tornadocash-decision-making-8db64014112> (U).
- Exhibit 71: (U) Website of Tornado Cash, "Ceremony," archived version from August 5, 2020, accessed via The Wayback Machine [REDACTED] available at <https://web.archive.org/web/20200805042602/https://ceremony.tornado.cash/> (U).
- Exhibit 72: (U) Website of FIOD "Arrest of suspected developer of Tornado Cash," August 8, 2022, available at: <https://www.fiod.nl/arrest-of-suspected-developer-of-tornado-cash/> (U).
- Exhibit 73: (U) Website of Investopedia, "USD Coin," September 27, 2022, [REDACTED] available at: <https://www.investopedia.com/usd-coin-5210435>. (U).
- Exhibit 74: (U) Website of Github, "Tornado-repositories/tornado-core Commits on March 24, 2022," [REDACTED] available at: <https://github.com/tornado-repositories/tornado-core/commits/master> (U).
- Exhibit 75: (U) Website of Medium "What is the xDai Chain and Why Should I Try It?" March 3, 2021, accessed October 6, 2022, available at: <https://medium.com/mycrypto/what-is-the-xdai-chain-and-why-should-i-try-it-40f539732fb4>

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE DECISIONAL AND DELIBERATIVE DRAFT~~

- Exhibit 76: (U) Website of DeCrypt, "What is Wrapped Bitcoin?" March 17, 2022, accessed October 6, 2022, available at: <https://decrypt.co/resources/what-is-wbtc-explained-bitcoin-ethereum-defi>. (U).
- Exhibit 77: (U) Website of Dune, "Tornado Cash Fees V04" [REDACTED] available at: <https://dune.come/queries/671343/124581> (U).
- Exhibit 78: (U) Website of MakeUseOf, "What is Software Forking," July 7, 2021, [REDACTED] available at: www.makeuseof.com/what-is-software-forking/ (U).
- Exhibit 79: (U) Website of Dune, "Introduction to Dune/Dune Docs," [REDACTED] available at: <https://docs.dune.com> (U).
- Exhibit 80: (U) Website of Github, "Github's Products" [REDACTED] available at: <https://docs.github.com/en/get-s-github/githubs-products> (U).
- Exhibit 81: (U) Website of CoinDesk, "How Bitcoin Mixers Work and Why People Use BitcoinMixers," January 18, 2022, [REDACTED] available at: <https://www.coindesk.com/learn/bitcoin-mixers-how-do-they-work-and-why-are-they-used/> (U).
- Exhibit 82: (U) Website of Council on Foreign Relations, "About CFR," [REDACTED] available at: cfr.org/about. (U).
- Exhibit 83: (U) Website of GitHub, "openzeppelin-contracts / contracts / proxy," [REDACTED] available at: <https://github.com/OpenZeppelin/openzeppelin-contracts/blob/master/contracts/proxy/Proxy.sol> (U).
- Exhibit 84: (U) Website of SPDX, "SPDX License List," [REDACTED] available at: <https://sodx.org/licenses/> (U).
- Exhibit 85: (U) Website of Forbes, "What is AVAX," September 16, 2022 accessed October 6, 2022, available at: <https://www.forbes.com/sites/qai/2022/09/16/avalanche-crypto-news-whats-going-on-with-the-scandal-surrounding-avax/?sh=66903beb6e8b>
- Exhibit 86: (U) Website of GitHub, "Tornado Repositories/Tornado Classic UI," [REDACTED] available at: <https://github.com/tornado-repositories/tornado-classic-ui/blob/master/LICENSE> (U).
- Exhibit 87: (U) Website of Medium, "Decentralizing TornadoCash: The Launch of TornadoFund and the Path Towards TornadoDAO," July 1, 2020, accessed September 21, 2022, available at:

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE DECISIONAL AND DELIBERATIVE DRAFT~~

https://medium.com/@Tornado_Fund/decentralizing-tornadocash-the-launch-of-tornado-fund-and-the-path-towards-tornadodao-a6d4ffc6c800
(U).

- Exhibit 88: (U) Website of OpenZeppelin, "Explore using OpenZeppelin," [REDACTED]
[REDACTED] available at: <https://docs.openzeppelin.com> (U).
- Exhibit 89: (U) Website of Crypto.com "Crypto Tokens vs Coins – what's the difference? June 20, 2022 [REDACTED] available at:
<https://crypto.com/university/crypto-tokens-vs-coins-difference>
- Exhibit 90: (U) Website of Etherscan, "Token Torn Token," [REDACTED]
available at:
<https://etherscan.io/token/0x77777feddddfc19ff86db637967013e6c6a116c#balances>. (U)
- Exhibit 91: (U) Website of Binance, [REDACTED] available at:
<https://www.binance.com/en>. (U).
- Exhibit 92: (U) Website of Binance, "List of Supported Assets- Binance.US, [REDACTED]
[REDACTED] available at: <https://support.binance.us/hc/en-us/articles/360049417674-List-of-Supported-Assets>. (U).
- Exhibit 93: (U) Website of Coinbase, "Compound Dai," [REDACTED]
available at: https://www.coinbase.com/price/compound-dai?__cf_chl_f_tk=D5VVEgmSWkF1fT7uFKgMSkvkGu8IEMSELpOHdXsjtR4-1664657609-0-gaNycGzNCZE#CompoundDaiCDAL. (U).
- Exhibit 94*: (U) Website of Tech Target, "Code Base," [REDACTED]
available at: www.techtarget.com/whatis/definition/codebase-code-base (U).
- Exhibit 95: (U) Website of Tech Target, "Source Code," [REDACTED]
available at: www.techtarget.com/searcharchitecture/definition/source-code (U).
- Exhibit 96: (U) Website of Etherscan, "Contract
0x58E8dCC13BE9780fC42E8723D8EaD4CF46943dF2," [REDACTED]
[REDACTED] available at:
<https://etherscan.io/address/0x58E8dCC13BE9780fC42E8723D8EaD4CF46943dF2> (U).
- Exhibit 97: (U) Website of CoinDesk, "Custodial Wallets vs Non-Custodial Crypto Wallets," March 9, 2022, accessed September 22, 2022, available at:
www.coindesk.com/learn/custodial-wallets-vs-non-custodial-crypto-wallets/
(U).

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

- Exhibit 98: (U) Website of Forbes, "Leaked 'Tai Chi' Document Reveals Binance's Elaborate Scheme To Evade Bitcoin Regulators," October 29, 2020, accessed September 22, 2022 available at: www.forbes.com/sites/michaeldelcastillo/2020/10/29/leaked-tai-chi-document-reveals-binance-elaborate-scheme-to-evade-bitcoin-regulators/?sh=3eff18812a92 (U).
- Exhibit 99: (U) Executive Order 13694, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," April 1, 2015. (U).
- Exhibit 100: (U) Executive Order 13722, "Blocking the Property of the Government of North Korea and the Workers' Party of Korea, and Prohibiting Certain Transactions With Respect to North Korea," March 18, 2016. (U)
- Exhibit 101: (U//~~FOUO~~) OFAC Memorandum for Record, "Analysis of TORNADO CASH Addresses and Contracts." (U//~~FOUO~~)
- Exhibit 102: (U) Website of Investopedia, "Tether (USDT): Meaning and Uses for Tether Crypto Explained, May 12, 2022, [REDACTED] available at: <https://www.investopedia.com/terms/t/tether-usdt.asp>. (U).
- Exhibit 103: (U) Website of Ethereum, "Intro to Ethereum," [REDACTED] available at: ethereum.org/en/developers/docs/intro-to-ethereum/. (U).
- Exhibit 104: (U) Thompson Reuters "Blockchain technology: Data Privacy Issues and Potential Mitigation Strategies," Resource ID: W-021-8235. (U).
- Exhibit 105: (U) Website of CoinMarket Cap, "Glossary – Annual Percentage Yield," [REDACTED] available at: <https://coinmarketcap.com/alexandria/glossary/annual-percentage-yield-apy>. (U).
- Exhibit 106: (U//~~FOUO~~) [REDACTED] (U//~~FOUO~~) [REDACTED]
- Exhibit 107: (U) Website of Ethereum, "Transactions," [REDACTED] available at: [ethereum.org/en/developers/d](https://ethereum.org/en/developers/docs/transactions/)
- Exhibit 108: (U) Website of Certik, "What is Blockchain Analysis? – Blog," [REDACTED] available at: certik.com/resources/blog/what-is-blockchain-analysis. (U).
- Exhibit 109: (U) Website of Certik, "About," [REDACTED] available at: certik.com/company/about. (U).

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

- Exhibit 110: (U) Website of Council on Foreign Relations, "Cryptocurrencies, Digital Dollars, and the Future of Money," updated September 24, 2021, [REDACTED] Available at: https://www.cfr.org/backgrounders/cryptocurrencies-digital-dollars-and-future-money?gclid=EAIaIQobChMI-b_uvai6-gIVk4vICh1BLAqHEAAYASAAEgLz%E2%80%A6. (U).
- Exhibit 111: (U) Website of Ethereum, "ERC-20 Token Standard," [REDACTED] Available at: ethereum.org/en/developers/docs/standards/tokens/erc-20/. (U).
- Exhibit 112: (U) Website of the Department of the Treasury, Press Releases, "Treasury Sanctions Russia-based Hydra, World's Largest Darknet Market, and Ransomware Enabling Virtual Currency Exchange Garantex," April 5, 2022. Available at: <https://home.treasury.gov/news/press-releases/jy0701>. (U).
- Exhibit 113: (U) Website of the Department of the Treasury, Press Releases, "Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups," September 13, 2019. Available at: <https://home.treasury.gov/news/press-releases/sm774>. (U).
- Exhibit 114: (U) Website of the Department of the Treasury, Press Releases, "U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats." May 6, 2022. Available at: <https://home.treasury.gov/news/press-releases/jy0768>. (U)
- Exhibit 115: (U) Website of Cointelegraph, "What are NFT's?" accessed August 25, 2022, available at: <https://cointelegraph.com/tags/nft> (U).
- Exhibit 116: (U) Website of Chainalysis, "Crypto Mixer Usage Reaches All-time Highs in 2022, With Nation State Actors and Cyber Criminals Contributing Significant Volume. July 14, 2022, [REDACTED] available at: blog.chainalysis.com/reports/crypto-mixer-criminal-volume-2022/. (U).
- Exhibit 117: (U) Website of the Department of the Treasury, "Frequently Asked Questions #561," March 19, 2018, accessed September 28, 2022. Available at: <https://home.treasury.gov/policy-issues/financial-sanctions/faqs/561>. (U).
- Exhibit 118: (U) Website of Ethereum, "Smart Contract Languages," August 22, 2022, [REDACTED] available at: <https://ethereum.org/en/developers/docs/smart-contracts/languages/#solidity>. (U).
- Exhibit 119: (U) Website of Tornado Cash, "jobs," [REDACTED] formerly available at: <https://tornado.cash/jobs/solidity-engineer>. (U).

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

- Exhibit 120: (U) Website of Tornado Cash, "Introduction," [REDACTED] captured August 5, 2022, available at: <https://web.archive.org/web/20220805205724/https://docs.tornado.cash/general/readme>. (U).
- Exhibit 121: (U) Website of Cointelegraph, "TORN soars 200% as Tornado.Cash's Governance token becomes tradable." February 9, 2021, accessed September 30, 2022. Available at: <https://cointelegraph.com/news/torn-soars-200-as-tornado-cash-s-governance-token-becomes-tradable>. (U).
- Exhibit 122: (U) Website of Tornado Cash, "Community Involvement," [REDACTED] available at: <web.archive.org/web/20220617060922/https://docs.tornado.cash/general/community-involvement>. (U).
- Exhibit 123: (U) Website of CoinDesk, "An Introduction to Sidechains," March 7, 2022, accessed September 30, 2022, available at: coindesk.com/learn/an-introduction-to-sidechains/. (U).
- Exhibit 124: (U) Website of Forbes, "What is Tether? How Does it Work?" accessed September 30, 2022, available at: forbes.com/advisor/investing/cryptocurrency/what-is-tether-usdt/. (U).
- Exhibit 125: (U) Website of Decrypt, "What is Wrapped Bitcoin?" May 17, 2022, accessed September 30, 2022. Available at: decrypt.co/resources/what-is-wbtc-explained-bitcoin-ethereum-defi. (U).
- Exhibit 126: (U) Website of CoinMarketCap, "What is Binance Smart Chain?" [REDACTED] available at: coinmarketcap.com/alexandria/article/what-is-binance-smart-chain. (U).
- Exhibit 127: (U) Website of CoinMarketCap, "About CoinMarketCap," [REDACTED] available at: <https://coinmarketcap.com/about/>. (U).
- Exhibit 128: (U) Website of Investopedia, "About Us," [REDACTED] available at: www.investopedia.com/about-us-5093223 (U).
- Exhibit 129: (U) Website of Investopedia, "Polygon (MATIC)," [REDACTED] 2022, available at: [https://www.investopedia.com/polygon-matic-definition-5217569#:~:text=Polygon \(MATIC\) is a cryptocurrency,such as Coinbase or Kraken](https://www.investopedia.com/polygon-matic-definition-5217569#:~:text=Polygon (MATIC) is a cryptocurrency,such as Coinbase or Kraken). (U).
- Exhibit 130: (U) National Institute of Standards and Technology, "Blockchain Technology Overview," October 2018. (U).

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

- Exhibit 131: (U) Website of Medium “Avalanche Mainnet is Live,” October 15, 2022, accessed September 30, 2022, available at: medium.com/avalancheavax/avalanche-mainnet-is-live-c2101c82ce10. (U).
- Exhibit 132: (U) Website of Tornado Cash, “Circuits,” [REDACTED] available at: web.archive.org/web/20220617060935/https://docs.tornado.cash/tornado-cash-classic/circuits. (U).
- Exhibit 133: (U) Website of Zcash, “What are ZK-SNARKs?” [REDACTED] available at: <https://z.cash/technology/zksnarks/>. (U).
- Exhibit 134: (U) Website of Tornado Cash, “Connect your wallet” [REDACTED] available at: web.archive.org/web/20220617060938/https://docs.tornado.cash/tornado-cash-classic/how-to-connect-your-wallet. (U).
- Exhibit 135: (U) Website of Tornado Cash, “Deposit & Withdraw -Tornado Cash,” [REDACTED] available at: web.archive.org/web/20220619102910/https://docs.tornado.cash/tornado-cash-classic/deposit-withdraw. (U).
- Exhibit 136: (U) Website of Tornado Cash, “Fund & Withdraw on Nova,” [REDACTED] available at: web.archive.org/web/20220617060939/https://docs.tornado.cash/tornado-cash-nova/fund-and-withdraw-on-nova. (U).
- Exhibit 137: (U) Website of Tornado Cash, “Shielded transfers on Nova – Tornado.Cash,” [REDACTED] available at: web.archive.org/web/20220617060938/https://docs.tornado.cash/tornado-cash-nova/shielded-transfers-on-nova. (U).
- Exhibit 138: (U) Website of Tornado Cash, “Anonymity Mining,” [REDACTED] available at: web.archive.org/web/20220617060938/https://docs.tornado.cash/tornado-cash-classic/anonymity-mining. (U).
- Exhibit 139: (U) Website of Tornado Cash, “How to Become a Relay?” [REDACTED] available at: web.archive.org/web/20220609181519/https://docs.tornado.cash/general/how-to-become-a-relayer. (U).
- Exhibit 140: (U) Website of Coinbase, “RPC Node,” [REDACTED] available at: <https://help.coinbase.com/en/coinbase/getting-started/crypto-education/glossary/rpc-node>. (U).

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

- Exhibit 141: (U) Website of Uniswap, "Introducing Uniswap V3," March 23, 2021, [REDACTED] available at: uniswap.org/blog/uniswap-v3. (U).
- Exhibit 142: (U) Website of BTCGeek, "How to Buy TORN Token from Tornado. ETH's most Trusted Privacy Protocol" February 9, 2021, [REDACTED] available at: <https://btcgeek.com/buy-torn-token-tornado/>. (U).
- Exhibit 143: (U) Website of Medium, "Introducing ppTORN: an Auto-compounding strategy for Tornado.cash \$TORN governance Staking. April 30, 2022, available at: medium.com/powerpool/introducing-pptorn-an-auto-compounding-strategy-for-tornado-cash-torn-governance-staking-1bd8d78e64a0. (U)
- Exhibit 144: (U) Website of AltcoinBuzz, "Make 61% APY with TORN on this Platform," May 11, 2022, [REDACTED] available at: <https://www.altcoinbuzz.io/passive-income/staking/make-61-apy-with-torn-on-this-platform/>. (U).
- Exhibit 145: (U) Website of Reuters, "Explainer: Ronin's \$615 Million Crypto Heist," March 30, 2022, accessed April 20, 2022. Available at: <https://www.reuters.com/technology/ronins-615-million-crypto-heist-2022-03-30/>. (U).
- Exhibit 146: (U) Website of Barron's, "Inside the \$625 Million Axie Hack and What it Means for Crypto Gaming," March 30, 2022, accessed April 29, 2022 available at: <https://www.barrons.com/articles/axie-infinity-hack-cryptocurrency-defi-gaming-51648671214>. (U)
- Exhibit 147: (U) Website of Reuters, accessed April 29, 2022, Available at: <https://www.reuters.com/>. (U).
- Exhibit 148: (U) Website of Barron's, "About," accessed April 14, 2022, Available at: <https://www.barrons.com/100-years-of-barrons/about>
- Exhibit 149: (U) Department of the Treasury, "Imposition of Sanctions Pursuant to Executive Order 13687 on January 2, 2015". (U).
- Exhibit 150: (U) Website of CoinDesk, "Twitters says 'Phone Spear Phishing' Let h ackers Gain employee Credentials," Updated September 14, 2022, accessed April 14, 2022, available at: <https://www.coindesk.com/markets/2020/07/31/twitter-says-phone-spear-phishing-let-hackers-gain-employee-credentials/>. (U).

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE DECISIONAL AND DELIBERATIVE DRAFT~~

- Exhibit 151: (U) Website of CoinDesk, "About," Accessed April 14, 2022, available at: <https://www.coindesk.com/about/>. (U).
- Exhibit 152: (U) Website of CoinTelegraph, "What is P2P trading, and how does it work in peer-to-peer crypto exchanges?" May 16, 2022, accessed September 30, 2022, Available at: cointelegraph.com/news/what-is-p2p-trading-and-how-does-it-work-in-peer-to-peer-crypto-exchanges. (U).
- Exhibit 153: (U//FOUO) [REDACTED] (U//FOUO) [REDACTED]
- Exhibit 154: (U) Website of Medium, "Validator Node FAQ," February 25, 2021, accessed April 29, 2022, Available at: <https://medium.com/centrality/validator-node-faq-154c728bac82#:~:text=Validators are node operators who,voting in the finalization protocol>. (U).
- Exhibit 155: (U) Website of Gnosis, "What is Gnosis Safe? Gnosis Help Center," [REDACTED] available at: <https://help.gnosis-safe.io/en/articles/3876456-what-is-gnosis-safe>. (U).
- Exhibit 156: (U) Website of Medium, "Getting to Know Third Party Validators," October 14, 2020, accessed April 29, 2022. Available at: <https://medium.com/stakefish/getting-to-know-third-party-validators-79b054b44ce7> (U).
- Exhibit 157: (U) Website of Ethereum, "Decentralized Autonomous Organizations," [REDACTED] available at: [tps://ethereum.org/en/dao/](https://ethereum.org/en/dao/). (U).
- Exhibit 158: (U) Website of CoinDesk, " This Elusive Malware Has Been Targeting Crypto Wallets for a Year," January 6, 2021, accessed April 29, 22, available at: <https://www.coindesk.com/tech/2021/01/06/this-elusive-malware-has-been-targeting-crypto-wallets-for-a-year/>. (U).
- Exhibit 159: (U) Website of the Federal Bureau of Investigation, "FBI Statement of the Attribution of Malicious Cyber Activity Posed by the Democratic People's Republic of Korea," April 14, 2022, available at: <https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-attribution-of-malicious-cyber-activity-posed-by-the-democratic-peoples-republic-of-korea>. (U).
- Exhibit 160: (U) Website of Tornado Cash, "FAQ," [REDACTED] available at: <https://tornado.cash/#faq>. (U)>
- Exhibit 161: (U) Website of Finance Brokerage, "Crypto Mixer Tornado Cash Won't Comply With Sanctions," March 11, 2022, [REDACTED]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

Available at: financebrokerage.com/crypto-mixer-tornado-cash-wont-comply-with-sanctions/. (U).

- Exhibit 162: (U) Website of Finance Brokerage, "About Us," [REDACTED] 2022, available at: financebrokerage.com/about-us/ (U).
- Exhibit 163: (U) Website of Bloomberg, "Crypto Funds From Ronin Breach Moved to Tornado Cash," April 4, 2022, accessed September 29, 2022, Available at: <https://www.bloomberg.com/news/articles/2022-04-04/hacker-move-stolen-crypto-funds-from-ronin-breach-to-obfuscator>. (U).
- Exhibit 164: (U//~~FOUO~~) OFAC Memorandum for Record, "Blockchain Analysis of TORNADO CASH." August 3, 2022. (U//~~FOUO~~)
- Exhibit 165: (U) Website of CoinDesk, "Tornado Cash Co-Founder Says the Mixer Protocol is Unstoppable," January 25, 2022, accessed May 4, 2022, available at: <https://www.coindesk.com/tech/2022/01/25/tornado-cash-co-founder-says-the-mixer-protocol-is-unstoppable/>. (U).
- Exhibit 166: (U) Website of CoinDesk, "Tornado Cash Adds Chainalysis Tool for Blocking OFAC-Sanctioned Wallets from Dapp," April 15, 2022, accessed September 29, 2022, available at: coindesk.com/tech/2022/04/15/tornado-cash-adds-chainalysis-tool-for-blocking-ofac-sanctioned-wallets-from-dapp/. (U).
- Exhibit 167: (U) Joint Cyber Security Advisory, "TraderTraitor: North Korean State-Sponsored APT Targets BlockChain Companies," April 18, 2022. (U).
- Exhibit 168: (U) United Nations Security Council, "Letter dated 27 August 2019 from the Panel of Experts established pursuant to resolution 1874 (2009) addressed to the President of the Security Council S/2019/691" August 30, 2019. (U).
- Exhibit 169: (U) Federal Bureau of Investigation, "Letterhead Memorandum 349F-CE-2200375," April 13, 2022. (U).
- Exhibit 170: (U) Vol. 87, No. 82 Federal Register 25352, April 28, 2022. (U).
- Exhibit 171: (U) Website of Bloomberg, "Hackers Steal about \$600 Million in One of the biggest Crypto Heists," March 29, 2022, available at: <https://www.bloomberg.com/news/articles/2022-03-29/hackers-steal-590-million-from-ronin-in-latest-bridge-attack#xj4y7vzkg>. (U).
- Exhibit 172: (U) Website of Crypto News Australia, "About Crypto News," accessed October 1, 2022, available at: <https://cryptonews.com.au/about>. (U).

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

- Exhibit 173: (U) Website of CoinDesk, "Why TVL Matters in DeFi: Total Value Locked Explained," accessed September 29, 2022, available at: <https://www.coindesk.com/learn/why-tvl-matters-in-defi-total-value-locked-explained/>. (U).
- Exhibit 174: (U) DPRK Cyber Threat Advisory, "Guidance on the North Korean Cyber Threat," April 15, 2020. (U).
- Exhibit 175: (U) Website of ImmuneFi, "Tornado Cash Bug Bounties," [REDACTED] available at: <https://web.archive.org/web/20220527111152/https://immune.fi.com/bounty/tornadocash/> (U).
- Exhibit 176: (U) Website of Crypto News Australia, "Tornado Cash Token (TORN) Surges 94% following Bullish Protocol Updates," March 5, 2022, accessed September 30, 2022, available at: <https://cryptonews.com.au/tornado-cash-token-torn-surges-94-following-bullish-protocol>. (U).
- Exhibit 177: (U) Website of Tornado Cash, "Tornado Cash smart contracts – Tornado.Cash" [REDACTED] available at: web.archive.org/web/20220617060935/https://docs.tornado.cash/general/tornado-cash-smart-contracts. (U).
- Exhibit 178: (U) Chainalysis, "The 2022 Crypto Crime Report," February, 2022. (U).
- Exhibit 179: (U) Attorney General's Cyber Digital Task Force, "Cryptocurrency Enforcement Framework," October, 2020. (U).
- Exhibit 180: (U) Website of Reuters, "U.N. Experts point finger at North Korea for \$281 million cyber theft, KuCoin likely Victim," February 29, 2021, accessed October 1, 2022, available at: <https://www.reuters.com/article/us-northkorea-sanctions-cyber/u-n-experts-point-finger-at-north-korea-for-281-million-cyber-theft-kucoin-likely-victim-id%E2%80%A6>. (U).
- Exhibit 181: (U//~~FOUO~~) OFAC Blockchain Analysis, "Blockchain Analysis of Tornado Cash and KuCoin Theft," October 1, 2022. (U//~~FOUO~~).
- Exhibit 182: (U) Website of Etherscan, "Contract 0xA160cdAB225685dA1d56aa342Ad8841c3b53f291," [REDACTED] available at <https://etherscan.io/address/0xA160cdAB225685dA1d56aa342Ad8841c3b53f291#code>. (U).
- Exhibit 183: (U) Department of the Treasury, "National Money Laundering Risk Assessment," February, 2022. (U).

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

- Exhibit 184: (U) Website of BeinCrypto, "Ethereum Name Service (ENS): Everything you Needs to Know," May 12, 2022, [REDACTED] available at: beincrypto.com/learn/ethereum-name-service-ens/. (U).
- Exhibit 185: (U) Website of Ethereum, "Layer-2," [REDACTED] available at: Ethereum.org/en/layer-2/. (U).
- Exhibit 186: (U) Website of Ethereum, "Sharding," [REDACTED] available at: Ethereum.org/en/upgrades/sharding/, (U).
- Exhibit 187: (U) Website of Investopedia, "What is Altcoin," updated May 16, 2022 [REDACTED] available at: <https://www.investopedia.com/terms/a/altcoin.asp#:~:text=Investopedia%20%2F%20Michela%20Buttignol-,What%20Is%20Altcoin%3F,from%20one%20of%20the%20two.> (U).
- Exhibit 188: (U) Website of Cointelegraph, "Venture Capital financing. A Beginners Guide to VC Funding the Crypto Space." Accessed October 2, 2022, available at: <https://cointelegraph.com/funding-for-beginners/venture-capital-financing-a-beginners-guide-to-vc-funding-in-the-crypto-space>. (U).
- Exhibit 189: (U) National Institute of Standards and Technology, "Blockchain Networks: Token Design and Management Overview," February 2021. (U).
- Exhibit 190: (U) Website of CoinTelegraph, "a Beginner's Guide to the BNB Chain: The evolution of the Binance Smart Chain," accessed October 2, 2022, available at: cointelegraph.com/altcoins-for-beginners/a-beginners-guide-to-the-bnb-chain-the-evolution-of-the-binance-smart-chain. (U).
- Exhibit 191: (U) Website of Investopedia, "What is Avalanche (AVAX)?" September 27, 2022, [REDACTED] available at: <https://www.investopedia.com/avalanche-avax-definition-5217374>. (U).
- Exhibit 192: (U) Website of Gnosis Chain, "Developers Overview," [REDACTED] available at: <https://docs.gnosischain.com/developers>. (U).
- Exhibit 193: (U) Website of CoinTelegraph. "Cryptocurrency On-Ramps and Off-Ramps, Explained," August 18, 2020, accessed October 3, 2020, available at: <https://cointelegraph.com/explained/cryptocurrency-on-ramps-and-off-ramps-explained>. (U).
- Exhibit 194: (U) Website of Binance, "Token Lockup," [REDACTED] available at: <https://academy.binance.com/en/glossary/token-lockup>. (U).
- Exhibit 195: (U) Website of Twitter, "Tornado Cash," August 23, 2019, accessed October 3, 2022, available at:

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE DECISIONAL AND DELIBERATIVE DRAFT~~

<https://twitter.com/tornadocash/status/1164903335532609537>. (U).

Exhibit 196: (U) Website of Decrypt, "Manifesto," Accessed October 5, 2022, available at: <https://decrypt.co/manifesto>. (U).

Exhibit 197: (U) Website of Immuta, "K-Anonymity: Everything You Need to Know," [REDACTED] available at: <https://www.immuta.com/blog/k-anonymity-everything-you-need-to-know-2021-guide/#:~:text=What%20is%20k%2DAnonymity%3F,that%20data%20can%20be%20obscured>. (U).

Exhibit 198: (U) Website of Tech Target, "Permissioned vs. permissionless blockchains: Key differences," [REDACTED] available at: <https://www.techtarget.com/blockchains/Permissioned-vs-permissionless-blockchains-Key-differences>.

Exhibit 199: (U) Website of Harvard Law School Forum on Corporate Governance, "An Introduction to Smart Contracts and Their Potential and Inherent Limitations," May 6, 2018, [REDACTED] available at: <https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/>

Exhibit 200: (U) Department of the Treasury, "National Proliferation Financing Risk Assessment," February, 2022. (U).

Exhibit 201: (U) Website of Etherscan, "Block #1400000," [REDACTED] available at: <https://etherscan.io/block/11400000>. (U).

Exhibit 202: (U) Website of Department of the Treasury, Press Releases, "U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash," August 8, 2022. Available at: <https://home.treasury.gov/news/press-releases/jy0916> (U).

Exhibit 203: (U) Website of Investopedia, "What is Decentralized Finance (DeFi) and How Does It Work?" [REDACTED] available at: [investopedia.com/decentralized-finance-defi-5113835](https://www.investopedia.com/decentralized-finance-defi-5113835). (U).

Exhibit 204: (U) Website of The Block.co, "Tornado Cash DAO votes to Take Partial Control Over Treasury Funds," August 12, 2022, [REDACTED] available at: theblock.co/post/163274/tornado-cash-dao-votes-to-take-partial-control-over-treasury-funds. (U).

Exhibit 205: (U) Website of the Department of the Treasury, Financial Sanctions, "Frequency Asked Questions #562," March 19, 2018, available at: <https://home.treasury.gov/policy-issues/financial-sanctions/faqs/562>. (U).

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE DECISIONAL AND DELIBERATIVE DRAFT~~

- Exhibit 206: (U) Website of Github, "Tornado Cash Core," available at: <https://github.com/tornadocash/tornado-core>. (U).
- Exhibit 207: (U//~~FOUO~~) Memorandum for Record, "Blockchain Analysis of Heists Using Tornado Cash," October 13, 2022. (U//~~FOUO~~).
- Exhibit 208: (U) Website of Github, "Roman Semenov," [REDACTED] available at: <https://github.com/poma?tab=overview&from=2019-11-01&to=2019-11-30>. (U).
- Exhibit 209: (U) Website of Github, "Tornadocash / Tornado-core, Commits" Page 1, [REDACTED] available at: https://github.com/tornadocash/tornado-core/commits/master?before=1ef6a263ac6a0e476d063fcb269a9df65a1bd56a+35&branch=master&qualified_%E2%80%A6. (U).
- Exhibit 210: (U) Website of Github, "Tornadocash / Tornado-core, Commits" Page 2, [REDACTED] available at: https://github.com/tornadocash/tornado-core/commits/master?after=1ef6a263ac6a0e476d063fcb269a9df65a1bd56a+34&branch=master&qualified_na%E2%80%A6. (U).
- Exhibit 211: (U) Website of Github, "Tornadocash / Tornado-core, Commits" Page 3, [REDACTED] available at: https://github.com/tornadocash/tornado-core/commits/master?after=1ef6a263ac6a0e476d063fcb269a9df65a1bd56a+69&branch=master&qualified_na%E2%80%A6. (U).
- Exhibit 212: (U) Website of Github, "Tornadocash / Tornado-core, Commits" Page 4, [REDACTED] available at: https://github.com/tornadocash/tornado-core/commits/master?after=1ef6a263ac6a0e476d063fcb269a9df65a1bd56a+104&branch=master&qualified_n%E2%80%A6. (U).
- Exhibit 213: (U) Website of Github, "Tornadocash / Tornado-core, Commits" Page 5, [REDACTED] available at: https://github.com/tornadocash/tornado-core/commits/master?after=1ef6a263ac6a0e476d063fcb269a9df65a1bd56a+139&branch=master&qualified_n%E2%80%A6. (U).
- Exhibit 214: (U) Website of Github, "Tornadocash / Tornado-core, Commits" Page 6, [REDACTED] available at: https://github.com/tornadocash/tornado-core/commits/master?after=1ef6a263ac6a0e476d063fcb269a9df65a1bd56a+174&branch=master&qualified_n%E2%80%A6. (U).

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

- Exhibit 215: (U) Website of Github, "Tornadocash / Tornado-core, Commits" Page 7, [REDACTED] available at: https://github.com/tornadocash/tornado-core/commits/master?after=1ef6a263ac6a0e476d063fcb269a9df65a1bd56a+209&branch=master&qualified_n%E2%80%A6. (U).
- Exhibit 216: (U) Website of Github, "Tornadocash / Tornado-core, Commits" Page 8, [REDACTED] available at: https://github.com/tornadocash/tornado-core/commits/master?after=1ef6a263ac6a0e476d063fcb269a9df65a1bd56a+244&branch=master&qualified_n%E2%80%A6. (U).
- Exhibit 217: (U) Website of Github, "Tornadocash / Tornado-core, Commits" Page 9, [REDACTED] available at: https://github.com/tornadocash/tornado-core/commits/master?after=1ef6a263ac6a0e476d063fcb269a9df65a1bd56a+279&branch=master&qualified_n%E2%80%A6. (U).
- Exhibit 218: (U) Website of Github, "Tornadocash / Tornado-core, Commits" Page 10, [REDACTED] available at: https://github.com/tornadocash/tornado-core/commits/master?after=1ef6a263ac6a0e476d063fcb269a9df65a1bd56a+314&branch=master&qualified_n%E2%80%A6. (U).
- Exhibit 219: (U) Website of General Services Administration, Digital.gov, "An introduction to GitHub," [REDACTED] available at: https://www.theregister.com/Profile/about_the_register/. (U).
- Exhibit 220: (U) Website of CoinDesk, "What Are Liquidity Pools?" June 7, 2022, accessed October 24, 2022, available at: <https://www.coindesk.com/learn/what-are-liquidity-pools/>. (U).
- Exhibit 221: (U) Website of Ethereum, "What is Staking?" [REDACTED] available at: <https://ethereum.org/en/staking/> (U).
- Exhibit 222*: (U) Website of NIST, "Glossary, Publishing Node," accessed October 24, 2022 <https://csrc.nist.gov/glossary/term/publithis> dushing_node#:~:text=Definition(s)%3A,%2C committing node%2C minting node.
- Exhibit 223: (U) Website of PCMagazine, "Encyclopedia, Off-Chain Governance," accessed October 24, 2022, available at: <https://www.pcmag.com/encyclopedia/term/off-chain-governance#:~:text=Modifications to a blockchain that, is how a DAO operates.> (U).

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~
~~PRIVILEGED / PRE-DECISIONAL AND DELIBERATIVE DRAFT~~

- Exhibit 224: (U) Website of PCMagazine, "About, " accessed October 25, 2022, available at: <https://www.pcmag.com/about>. (U).
- Exhibit 225: (U) Website of Elliptic, "the \$100 Million Horizon Hack: Following the Trail Through Tornado Cash to North Korea," July 13, 2022, available at: hub.elliptic.co/analysis/the-100-million-horizon-hack-following-the-trail-through-tornado-cash-to-north-korea/. (U).
- Exhibit 226: (U) Website of Gemini, "Crypto Wallets, Custodial vs Non-Custodial," updated May 6, 2021 [REDACTED] available at: <https://www.gemini.com/cryptopedia/crypto-wallets-custodial-vs-noncustodial/> (U).
- Exhibit 227: (U) Website of Gemini, "About," [REDACTED] available at: <https://www.gemini.com/about>. (U).
- Exhibit 228: (U) Website of PCMagazine, "Encyclopedia, pseudo-random," accessed November 1, 2022, available at: <https://www.pcmag.com/encyclopedia/term/pseudo-random-numbers>. (U).
- Exhibit 229: (U) Website of GitHub, "Creating a Repository," [REDACTED] available at: <https://docs.github.com/en/get-started/quickstart/hello-world>. (U).